SPECIAL EDITION

VOLUME 7 ◆ NUMBER 1 WINTER 2022

THE CYBER DEFENSE REVIEW

Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020

Editors
Chris C. Demchak and *Francesca Spidalieri*

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

⋄ Special Edition ⋄

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

CONTACT
Army Cyber Institute
Spellman Hall
2101 New South Post Road
West Point, New York 10996

SUBMISSIONS
The Cyber Defense Review
welcomes submissions at
mc04.manuscriptcentral.com/cyberdr

WEBSITE
cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.
The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

THE CYBER DEFENSE REVIEW VOLUME 7 ◆ NUMBER 1 ◆ WINTER 2022

SPECIAL EDITION

Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020

EDITORS

Chris C. Demchak and Francesca Spidalieri

FORWARD

INTRODUCTION

STRATEGY UNLEARNED LESSONS

NATIONAL CAPACITY UNLEARNED LESSONS

THE CYBER DEFENSE REVIEW VOLUME 7 ◇ NUMBER 1 ◇ WINTER 2022

SPECIAL EDITION

POLICY AND ORGANIZATION UNLEARNED LESSONS

SOCIO-TECHNICAL-ECONOMIC SYSTEMS (STES) UNLEARNED LESSONS

CONCLUSION

FORWARD

The Cyber Defense Review: Addressing Critical Unlearned Lessons

Colonel Jeffrey M. Erickson

SPECIAL EDITION

VOLUME 7 • NUMBER 1

WINTER 2022

THE CYBER DEFENSE REVIEW

Unlearned Lessons from the
First Cybered Conflict Decade, 2010-2020
Editors
Chris C. Demchak and *Francesca Spidalieri*

Strategy – Unlearned Lessons
Catherine Lotrionte, James A. Lewis, Nigel Inkster, Chris Spirito

National Capacity – Unlearned Lessons
Sandro Gaycken, Edward C. Cardon, TJ White, Benjamin Ang
Eviatar Matania and Lior Yoffe

Policy and Organization – Unlearned Lessons
Emily O. Goldman, Harvey Rishikof,
Michael Klipstein and Palo Breuer, Andrea Little Limbago

Socio-Technical-Economic Systems (STES) – Unlearned Lessons
Chris Demchak, Dan Geer, Sam J. Tangredi, Sean Kanuck
Yuval Shavitt and Chris C. Demchak, John T. Harvey

FORWARD
Addressing Critical Unlearned Lessons — *Col. Jeffrey M. Erickson*

INTRODUCTION
Tallying Unlearned Lessons from the
First Cybered Conflict Decade, 2010-2020 — *Chris C. Demchak*, *Francesca Spidalieri*

CONCLUSION
When Experience Speaks and Too Few Listen –
Curating the Unlearned Lessons — *Chris C. Demchak*, *Francesca Spidalieri*

ARMY CYBER INSTITUTE • WEST POINT

Welcome to a unique Special Edition of *The Cyber Defense Review* (CDR). For the last decade, those who have worked in the cyberspace domain will likely agree that some persistent issues and problems continue to be debated with no clear resolution. These include ideas and solutions that may have been identified but did not gain the necessary traction to achieve positive outcomes. This issue focuses on those "Unlearned Lessons" from the last decade with the intent of encouraging action.

The variety of topics covered in the special edition are wide. In this issue, you will find articles on diplomacy, international relations, adversaries, alliances, emerging threats, economics, and beyond. These are not just technical issues, but also societal and governmental challenges exacerbated through the dramatic nature of cyber technology. Each article is kept intentionally short and to the point for maximum effect.

It is also worth pointing out that just because the US may not have learned these lessons, our adversaries may not be in the same situation. Differences in government, priorities, and cultures may not be a hindrance to our adversaries. The "Unlearned Lessons" may have given our adversaries a first-mover advantage in the cyberspace domain, which further increases the need for us to consider, understand, and potentially act on these topics.

The special edition authors represent a diverse group of leaders from the cyberspace domain. They have all dedicated a significant portion of their professional careers wrestling with these challenging issues, and it is prudent that we all think about what they are saying. When these authors speak, it is incumbent upon members of government, the military, academia, and industry to take the time and pay heed to their words.

Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

A special thank you to Dr. Chris Demchak (Naval War College) and Prof. Francesca Spidalieri (University of Maryland) as the Guest Editors for crafting this critically important issue. Their time and effort in making this issue a success and a must-read for the community are apparent throughout.

We hope that continued dialogue with key leaders in the community will lead to decisive action. As much as I look forward to future issues of the CDR, I hope that we do not have to see a "*Lessons (Still) Unlearned from the Second Decade of Cyber Conflict*" special edition ten years from now. We can avoid ending up with that future issue by turning the page, considering the thoughtful points made by these authors, and then working to address these challenges within the larger community.

Introduction

Tallying Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020

Chris C. Demchak
Francesca Spidalieri

The world is now ten years into the age of overt cybered[1] conflict. The "Cyber Westphalian" world is well past infancy, and the newly conflictual world arena faces emerging great power competition across all domains. It is time to tally up the learning.

These essays engage that challenge with a twist. They look at what was missed, ignored, mistaken, or simply not learned despite the indicators and experience. This issue reflects most of a conversation held at the U.S. Naval War College in November 2020 where a small group of senior cyber and security practitioners and scholars met for three half-days to share and discuss the lessons of the first decade of cybered conflict. Included among the attendees were former commanders of the various U.S. cyber commands, as well as senior scholars of international relations with considerable cyber research experience. Others averaged a decade or several in involvement with and study of cyberspace, cybered conflict, and cyber campaigns.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

[1] "Cybered" is an adjective indicating the spectrum of effects from cyberspace as it acts, enables, or operates through the wider socio-technical-systems of a modern society. Developed first in 2011 as part of the term "cybered conflict," it was meant to indicate a broader range of conflict beyond the networks and struggles between states and groups ranging from peace to war. Today, while the term "cyber" used alone encompasses the universe of artifacts and effects associated with the rising thoroughly digitized world, the term "cybered" is still necessary to indicate effects beyond digitization – a more comprehensive view. One might say the 'digitized world' is a more neutral and even innocent framing of what has happened with the onset of the current era, while the "cybered world" clearly points to the rise of great power and now Great Systems Conflict. See Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (March 1 2011). Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

Unlike other workshops, the charge was not to list successes but to uncover failures to learn across the US and its democratic allies. The meeting, titled "'Entre Nous – Blunt Lessons of Cyber Strategy and Stability," focused on identifying the overlooked, underappreciated, or novel strategic and organizing lessons that still needed to be – or never had been – recognized. The workshop concluded with discussions of what was needed to have these unlearned lessons recognized and implemented across Western democracies going forward. The organizing hosts were the NWC's Hopper Chair of Cyber Security (Chris Demchak) and Leidos Chair of Future Warfare Studies (Sam Tangredi), both part of the Cyber and Innovation Policy Institute, and the co-hosts were the European School of Management's Digital Society Institute Director (Sandro Gaycken) and the Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center Research Director (Lior Tabansky). Together, the organizers sought to change up the discussion to stimulate a wider view of what was missed over an incredible ten years of learning about cyber conflict and the rising of the digitized Great Systems Conflict in the waning Westernized global system of a post-Cold War unipolar world.

The results of the discussion's attendees and several additional well-known cyber experts are captured in this collection of essays on unlearned lessons over the past decade. There are four sections that begin with the highest level of generality (strategy and key actors), move to more national capacity issues, then to policy and organizational oversights, and finally roll broadly to the systemic questions transcending all levels. The sections are titled accordingly: Unlearned Strategy Lessons, National Capacity Lessons, Policy and Organizational Lessons, and Socio-Technical-Economic Systems (STES) Lessons. Each section presents three to five distinct discussions of one or more lessons unlearned or missed and the way forward.

Francesca Spidalieri is an Adjunct Professor for Cyber Policy at the University of Maryland's School of Public Policy and works as a cybersecurity consultant for Hathaway Global Strategies, LLC. She is also the Co-Principal Investigator for the Cyber Readiness Index 2.0 project at the Potomac Institute for Policy Studies, and the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University. In addition, Francesca serves as a cybersecurity subject-matter expert for the World Bank, the Global Forum on Cyber Expertise, the UN International Telecommunications Union, the EU CyberNet, and several other research institutes in Europe. Her academic research and publications have focused on cyber leadership development, cyber risk management, digital transformation, and national cyber preparedness and resilience. She lectures regularly at cyber-related events in the United States and Europe and contributes to journal articles and other publications on cybersecurity matters affecting countries and organizations worldwide.

The arguments are based on the experience, research, and observations of these senior cyber and national security experts.

The purpose is to identify the shortcomings in as crisp a manner as possible to stimulate critical thinking in the readers and, one hopes, direct action on the part of those involved in policy, strategy, and leadership positions. Therefore, the essays are short. While the collection is equally intended for the use of scholars, practitioners, and students, it is not meant to be a deeply academic aggregate arguing with other publications, scholars, or pundits. Rather, its central purpose is to bring forward these lessons in as brief and yet persuasive a form as possible to make them useful for today's policy, strategy, or classroom discussions.

After ten years of experiments in creating organizations, strategies, policies, and campaigns for, through, and enabled by cyberspace, it is important to know what of value in lessons to be learned has nonetheless been neglected or missed in reality. The fervent hope of these authors, the editors, and those who attended that discussion twelve months ago is that this collection will interest security studies communities, strategic analysts, cybersecurity specialists, and service members as well as upper-division students and generalists. It will be accessible and yet have enough depth to guide education and stimulate curiosity and research questions. Some essays will contain some controversial observations and corresponding conclusions. These need to be refracted through future national strategies, policies, and institutional lenses for the future lest the unlearned lessons contribute to hard, painful lessons in strategic failures in the rising deeply cybered, post-Westernized, authoritarian world.

No edition of any journal can occur without the considerable help of those who made it possible. In our case, that support begins with the germinating workshop itself. First and foremost, the generous support and insightful thinking of the U.S. Naval War College's Leidos Chair of Future War Studies, Dr. Sam Tangredi, enhanced the discussion and focus throughout the meeting. Our allied co-hosts, Dr. Sandro Geycken of the European School of Management's Digital Society Institute (ESMT/DSI) and Dr. Lior Tabansky of Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center (BICRC), provided the necessary alternative views to widen the thinking of the attendees and the offerings in this special issue. That support is and was deeply appreciated and will be sought – along with the presence of these eminent scholars – in future meetings. Beyond the academics and the practitioners are the critical staff members whose innovative and energetic support turned yet another virtual workshop into one that felt "intimate" and collegial, according to one senior attendee. Key members were Andrea Gonzales and David Bolender, both of whom are now a part of the ongoing team for all future Hopper-Leidos Chairs' Strategic Dialogues.

This special issue is not the last to address what a decade of experimentation might have missed or what ten years of evolution might have gotten wrong. Yet, it is an unusual issue in that everyone participating in the collection has been in the cyber security community with a close-up view the entire time. A number of them were in the position to make or debate important decisions. For many, the lessons identified as unlearned are quite close to personal experiences, and their professional concerns that we do not continue to neglect to learn is deeply held. We all hope this issue will spark reconsideration, open up some debate, and help reveal alternative future paths. We only have one world, and we are moving very fast toward its next and already more conflictual iteration. It is time to make sure we are noting the missteps before it is too late to correct them in the future.

NOTES

Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).

Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (March 1, 2011): 31-62.

Strategy
Unlearned Lessons

Bringing the Law In: Unlearned Lessons for Diplomats and Others

Dr. Catherine Lotrionte

INTRODUCTION

For over twenty years, “developments in the field of information and telecommunication in the context of international security” has been on the agenda of the United Nations (UN). In 2003, the UN General Assembly established the first formal group of governmental experts (UN GGE) to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. From the beginning of this process, the role of international law has been part of the discussions about existing threats in cyberspace and what measures could be taken to minimize those threats. Indeed, at the conclusion of the first UN GGE in 2004, the Chairman explained that the group was unable to conclude a consensus report because, among other reasons, there were “differing interpretations of current international law in the area of international information security.”[1] Since the conclusion of this first UN GGE, there have been six more GGEs, with the last one wrapped up in May 2021. Each of these groups were tasked with studying the potential threats from State malicious actions in cyberspace and how international law applied to such State actions, among other topics. In 2018, to expand the representation of States involved in the study, a parallel process–the Open-Ended Working Group (OEWG) on Information and Communication Technology Developments in the Context of International Security–was established at the UN. It is fully composed of UN members. The OEWG was directed to study, among other issues, how international law applies in cyberspace. On March 12, 2021, the OEWG adopted its Final Substantive Report.

These discussions and negotiations have gone on for nearly twenty years and yet, there has been no consensus on what specific rules of international law apply in cyberspace, never mind how they might apply in specific circumstances. Rather, the only consistent agreement in the combined reports of the GGEs and OEWG (the UN Reports) has been that

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Dr. Catherine Lotrionte is a Senior Researcher at Georgetown University where she teaches international law and national security law, a Senior Associate in the Technology Policy Program at CSIS, and a Senior Fellow at the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. Previously she served as the Brent Scowcroft scholar at the Atlantic Council. She is the Founder and former Director of the CyberProject at Georgetown University. Dr. Lotrionte has served as Counsel to the President's Foreign Intelligence Advisory Board at the White House and as an Assistant General Counsel at the Central Intelligence Agency. She has a JD from New York University Law School and a MA and Ph.D. from Georgetown University.

"international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security, and stability in the ICT environment." Even with respect to what appears to be a modest agreement on the applicability of one treaty, the UN Charter, in cyberspace, disagreement remains between the States over what provisions of the Charter apply. For example, some States have objected to the inclusion of the Charter's Article 51 on self-defense within the reports, notwithstanding the right of self-defense is part of customary international law, pre-existing the Charter. Indeed, the OEWG's ninety-one page "Compendium of statements in explanation of position on the final report" ("Compendium") released on March 25, 2021, reveals the numerous disagreements States continue to have related to specific rules of international law and their applicability to cyberspace.

While there are numerous lessons that negotiators have learned throughout this process, there are lessons about the role of international law in establishing a more stable cyberspace that the diplomats involved in the UN processes seem to have missed. Based on a careful reading of the record, those involved in negotiating and drafting the reports have failed to understand the nature of international law, including how it is created and how it develops. As the renowned international lawyer and former State Department official Louis Henkin once wrote, "Lawyer and diplomat . . . are not even attempting to talk to each other . . . it seems unfortunate, indeed destructive, that they should not, at the least, hear each other."[2] Unfortunately, it seems, as Henkin pointed out, that international lawyers and diplomats were not speaking, at least enough, to each other during the UN processes leading to confusion among States, contradictory understandings about the law, and a lack of agreement on the applicability of international law in cyberspace. In seeking to address this problem, this essay will outline the nature of international law before identifying specific aspects of the reports that could have been clearer given a deeper understanding of international law. The hope is that this essay may facilitate a dialogue between the lawyers and the diplomats that can lead to a more sophisticated view of international law, what it is, how it is made, and the role it can play in establishing a more stable, open, and interoperable cyberspace.

INTERNATIONAL LAW

Customary International Law

A useful starting point for the examination of the nature of international law begins with the traditional theory of sources of international law recognized in Article 38 of the Statute of the International Court of Justice (ICJ): treaties, custom, and general principles. Although even this list is not complete, given the limited space, this essay will only address the first two main sources: treaties and custom. There is no hierarchy between these two sources of law with both considered just as legally binding. Customary law is the oldest source of international law, the one which generates rules binding all States except for persistent objector States. It is the most difficult to identify at times, and a source not addressed in the UN Reports. Once an international law has been developed, whether through a treaty or customary practice that is accepted as law, if a State violates the law, international responsibility will result, and that State is obligated to stop its violation of the law and make any reparations for the harm that its violation may have caused. This contrasts with norms which are not legally binding so when they are violated, do not result in State responsibility for any wrongful act under international law. Although norms are not legally binding, those norms can develop into legally binding law if, for instance, a State negotiates a treaty incorporating the norm into the agreement or through the development of customary law.

Unlike treaty law, customary law is not a written source and, in order to determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice by States that is accepted by those States as law. In other words, customary law first develops through the widespread and consistent State practice and, secondly, when the practice in question is undertaken with a sense of legal right or obligation (*opinio juris*) as distinguished from a general practice that is undertaken as a habit or mere usage.These two elements, practice and *opinio juris*, have to be separately ascertained and are necessary in order for a rule of customary international law to exist.

The relevant practice for a customary law consists of conduct of the State, whether in the exercise of its executive, legislative, judicial, or other functions that can include both physical and verbal acts as well as inaction, under certain circumstances. Examples can include conduct of States in connection with resolutions adopted by an international organization (e.g., UN GA resolutions) or at an intergovernmental conference (e.g., UN GGE meetings); executive conduct including operational conduct on the ground; legislative and administrative acts and decisions of national courts. While the practice does not have to be universal or perfectly consistent, it must be sufficiently widespread and representative as well as consistent. A short period of time is not necessarily a bar to the development of the necessary practice; if the practice is widespread there is no requirement that the practice must be for a specific duration of time.

Evidence of a practice's acceptance as law may take a variety of forms including public statements made on behalf of States; official publications; government legal opinions; diplomatic correspondence; decisions of national courts; treaty provisions; and conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference. While resolutions of international organizations or international conferences cannot themselves create a rule of customary international law, they can provide evidence and content of a rule of customary international law or contribute to its development. Furthermore, failure to react over time to a practice may serve as evidence of acceptance as law provided that States were in a position to react, and the circumstances called for some reaction.

Once a customary rule exists it binds all States, including those States that did not participate in the practice that led to the crystallization of the custom, subject only to what is known as the "persistent objector" principle. According to the persistent objector principle, a State that has persistently rejected a new rule as it was developing can avoid its application, as long as the objection was made known to other States clearly and persistently. Lastly, it is possible to have a rule of particular customary international law whether regional, local or other if there is a general practice among the States concerned that is accepted by them as law.

Treaty Law

According to the customary rule of international law of *pacta sunt servanda*, States are required to honor their agreements. As such, treaties, which are agreements between States and sometimes between States and international organizations, are a source of legal obligations under international law and legally binding on all parties to the agreement. The Vienna Convention on the Law of Treaties is the relevant law that applies to the formation, application, and interpretation of international agreements. Although not adopted by all States, most of its provisions are considered reflective of customary international law. Historically, some of the most challenging aspects of treaty law has been over the interpretation of treaty provisions that are at times vague and ambiguous. In some areas of State practice where activities are relatively new, there may not have been enough time and practice for States to conclude that a treaty regulating the activities was necessary. At other times, States may prefer that the activities remain unregulated by a new treaty or that the activities are already regulated by an existing treaty. In either case, the lack of a specific treaty covering particular activities does not mean there is no existing international law that regulates those activities. There may be other treaties applicable to those activities as well as customary international law.

Treaties can give rise to rules of international law in at least three ways. First, they can create specific rules of law that bind the parties to the treaty. Second, they can codify existing rules of customary law. For example, the inherent right of self-defense is codified in Article 51 of the UN Charter. The legal doctrine of self-defense is an ancient doctrine of international law that pre-existed the UN Charter. In more recent time, the contours of the customary right of self-defense were restated in the 1841 correspondence over the sinking of the *Caroline*. In that case, the negotiators recognized for force to be lawfully undertaken in self-defense, two criteria had to be met: 1) necessity and 2) proportionality. These two criteria have continued to inform contemporary understandings of Article 51.

Third, treaties can establish a specific rule for the parties that evolves into a general rule of customary international law. Take, for example, the Article 2(4) prohibition on the use of force in the UN Charter. Prior to the adoption of the Charter in 1945, there was no rule of customary law specifically prohibiting the use of force. In fact, States maintained the right to use force as a legitimate tool of foreign policy. While the Kellogg-Briand Pact of 1928 sought to outlaw war as an instrument of national policy, it did not seek to outlaw all uses of force. The UN Charter, however, explicitly created a prohibition against the use of force. At the time the Charter was adopted, only those States that ratified the Charter were bound by that obligation as a matter of treaty law.

Since 1945, the prohibition on the use of force embodied in Article 2(4) has become customary international law. This is because there has been both widespread State practice consistent with the rule of Article 2(4) and affirmative assertions by States that the use of force prohibition in Article 2(4) is a legal obligation. Indeed, the International Court of Justice (ICJ) has repeatedly recognized that this treaty-based rule has ripened into a universal customary rule of law. As a consequence, even non-signatories to the UN Charter treaty would be bound by the prohibition on the use of force in Article 2(4) as a matter of customary international law.

THE UN REPORTS: WHAT THEY REVEAL

The UN Reports' lack of clarity on the terminology used has led to much confusion about what exactly the negotiators were in agreement about. For instance, despite the fact that the two groups (i.e., GGE & OEWG) were tasked to study relevant concepts, including norms, rules and principles and international law, these terms were never defined. This section identifies a few of the instances that may have contributed to confusion and the lack of progress in the study of the role of international law in this context.

Beginning with the 2013 UN GGE report, there was no clear distinction drawn between the non-binding voluntary norms outlined and the binding international rules identified within the report. Indeed, the 2013 report included both norms and international law under the same heading, titled "Recommendations on norms, rules and principles of responsible behavior by States." Including a reference to the UN Charter treaty within a section on voluntary norms may have been the initial indication that the experts did not fully recognize the nature of treaty or customary law. Oddly, paragraph 23 within this same section, dealing with norms, rules and principles, asserts that, "States must meet their international obligations regarding internationally wrongful acts attributable to them." While this is potentially a reference to the customary law of State responsibility, it is unclear what this language means or why it would be included under a section dealing with voluntary norms. Apparently, in trying to clarify the difference between norms and law, both the 2015 UN GGE report and the OEWG report noted that norms were not intended to replace international legal obligations owed by States.

The fourth UN GGE meeting, from 2014-2015, had a new task formally added to its official mandate: to study how international law applies to the use of information and communications technologies by States. The group's final report included a new section at the end titled, "How international law applies to the use of ICTs." This section reiterated the applicability of international law and the UN Charter, specifically, to cyberspace. In paragraph 28 of this section, the report provides "non-exhaustive views on *how* international law applies to the use of ICTs by States." Here the report indicates that "the Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction . . ." Although these principles are part of well-established, binding customary international law, the report indicates that the group merely "noted" them as compared to other instances in this section where the group stated that "States must observe" other principles of international law.

Listed within the norms, rules and principles section of the 2015 UN GGE report are general descriptions of customary international laws, but the report does not use the rules' legal terminology. For example, in this section that report notes, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." This describes the principle of due diligence under international law. The section also mentions the legal obligation to not conduct or knowingly support activities that damage the critical infrastructure within another country. The section identifies these obligations as norms that are voluntary and non-binding, explaining that norms do not limit or prohibit action that is consistent with international law. It uses the word "should" to indicate the non-binding nature of the norms. Including these legally binding obligations within this section, with no explanation as to why, creates confusion about the meaning of the legal rules and how they are understood by those negotiating the terms of the report.

In seeking to draft a consensus report in 2017, the fifth UN GGE tried to navigate disagreements among that States about the applicability of specific international rules, including the law of self-defense, the law of countermeasures, and international humanitarian law. Ultimately, the group was unable to produce a final consensus report in 2017. In view of the perceived failure of the fifth GGE to reach a consensus, a parallel process, including all interested UN Member States, was proposed at the UN. The establishment of the new OEWG in 2018 meant that there would be two parallel UN processes that were tasked with studying how international law applied to the use of information and communications technologies by States.

On March 12, 2021, the OEWG adopted its Final Substantive Report. The Final Report acknowledged and supported the previous consensus reports of the GGE, although with some differences in language and not including several international legal principles that were included in the 2015 GGE report. While called a breakthrough by some, as far as the clarification of the applicability of international law, it would be a reversal of what limited progress on the topic had been made during the 2013 and 2015 GGE negotiations. The seeming confusion about the nature of international law generated through the UN GGE process and reflected in the reports may have contributed to the fact that the sole reference to international law in the OEWG report is the same reference made in the 2013 UN GGE report that "international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment." Notably, the OEWG report does not specify in any detail what rules of law the States agreed were applicable in cyberspace.

THE PRACTICE OF STATES

As the OEWG report concluded, further common understanding about how international law applies to State use of ICTs is needed. To be able to do this, however, diplomats tasked with studying how international law applies in this space need to fully understand the very nature of the law and how it develops. One important aspect of the development of international law, and in particular, of customary international law, as stated above, is the practice of States. Therefore, diplomats also must understand the practice of States in cyberspace as they assess the applicability of international law, and in particular, customary international law. In other words, those involved in the UN processes ought to be cognizant of the State practice that has been taking place in cyberspace over the last decades. It is through such State practice, coupled with *opinio juris,* that customary international law develops. Indeed, where there has been extensive State practice in cyberspace with States publicly attributing malicious cyber activity to other States and invoking international law, customary rules can crystalize and therefore, such practice needs to be part of any international discussions about intentional law and cyberspace.

For instance, in 2018, the United Kingdom accused Russia of a "flagrant violation of international law" for carrying out a "campaign of cyber-attacks" that included the disruption of transport systems in Ukraine. In 2020, Russia was accused of violating international law in a 2019 cyber-attack on Georgia that knocked out the national TV station and government websites. Because of these attacks, in March 2020, for the first time the issue of cyber-attacks was raised as a separate issue that threatened international peace and security at the UN Security Council. Estonia, the United States, and the United Kingdom condemned the "widespread disruptive" cyber-attacks by the Russian military service, GRU, that were part of Russia's broader campaign of hostile and destabilizing activity against Georgia. In cases such as these, where States have indicated their position on malicious cyber activities violating international law, it is incumbent on diplomats negotiating agreements related to cyber activities and international law to understand the relevance of such State practice and its role in the confirmation of, or development of, customary international law. Furthermore, just as importantly, are those occasions when States engage in malicious cyber practices and other States do not articulate any violation of international law.

CONCLUSION

The OEWG Compendium makes clear that there were disagreements over the final language in the report by the States. Related to international law, some States objected to the lack of specificity of international rules within the report while others expressed concern over confusion and lack of clarity about international rules. These concerns may explain why the Final Report could go no further than to simply reaffirm that, in cyberspace, international law and the UN Charter apply.

According to the diplomat George Kennan, the role of diplomacy was to facilitate change as it occurred in the world environment. According to Kennan, international law was "too abstract, too inflexible, too hard to adjust to the demands of the unpredictable and the unexpected . . . ."[3] Writing in 1951, Kennan viewed international law as not useful for the tasks of the diplomat that involved a nation's vital interests and military security. Kennan may have mistakenly been focusing only on some stultified concept of international law and not on the way in which international law develops through State practice to meet the needs of States in ensuring the peace and security of the international community. Irrespective of why Kennan had this critical view of the role of law in diplomacy, this cynical "realism" about international law does not reflect the facts of international life.

Today, diplomats and other foreign policy makers must necessarily recognize international law as important to their tasks. Indeed, the cyber diplomats have done so by their attempts to include the role of the law in regulating States' use of ICTs. The narrow view of international law, however, that has dominated the UN discussions on cyberspace has neglected important lessons about State practice and international law over the last couple of decades as States have developed cyber capabilities and used them in their international relations. The fruitful next steps for all of these cyber diplomats ought to include a thorough review and understanding of the nature of international law, its creation and development, and how it is applicable in the cyberspace context, given the practice of States.

NOTES

1. Rauchhaus, R., Evaluating the Nuclear Peace Hypothesis:A Quantitative Approach, Journal of Conflict Resolution, Vol. 53, IMr. Krutskikh, A/C.1/60/PV.13, 5, October 17, 2005, https://undocs.org/pdf?symbol=en/A/C.1/60/PV.13.
2. Louis Henkin, How Nations Behave: *Law and Foreign Policy* 4 (1979).
3. George Kennan, *American Diplomacy*, 1900-1950, 99 (1952).

Private Actors' Roles in International Cybersecurity Agreements – Unlearned Lessons

Dr. James Lewis

Vocal communities in the West demand a role in international public policy for cyberspace. In some areas of activity, such as privacy, controls on social media content, commercial issues like anti-trust or digital taxation, this private sector involvement is essential. But the unlearned lesson is that it is equally important for national security, as is the effective negotiation on security, which is still the purview of states.

One reason for these demands is the erosion of the clear division between internet security and internet governance. Internet governance has been the domain of a multistakeholder community. The members of the multistakeholders community increasingly expect to play a similar role in questions of international cybersecurity. Conversely, most governments had been content to leave internet governance to civil society and corporations, but now, as governance affects their economies and safety, some want a more prominent or even guiding role in the digital world. This confluence - it could even be described as a collision - over roles and responsibilities is complicated by China and Russia's differing visions for security, data governance, and sovereignty. The tensions between multistakeholders and government and between democracy and authoritarian views of digital governance complicate the discussions of the role of the private sector.

To draw upon precedent, in 1915, when it became clear that World War One would not end anytime soon, a wealthy American business leader, Henry Ford, launched a peace initiative. He bought a ship, filled it with pacifists, ministers, and academics (creating the ancestor of the multistakeholder community), and set sail for Europe to persuade the combatants to embrace peace. The warring powers did not warmly receive Ford's well-intentioned effort. At best, they considered him naive. Media coverage in the US was

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

critical, sarcastic, and openly hostile in London, Paris, and Berlin. The fate of the well-intentioned Peace Ship is a precedent for proposals to create Cyber Peace or a Digital Geneva Convention.

It is not a perfect precedent, however, because of political changes since 1915. One difference is a perception in democratic societies that cyberspace is too important to be entrusted solely to states, but the more important change is how states use coercion in cyberspace. Cyberconflict is a central battle zone in the new conflict between democracies and authoritarians, and certainly, the authoritarians have no intention of forsaking this battle.

It's worth noting that having non-governmental actors renounce cyberwar and cyber "weapons" is like having vegetarians agree to renounce meat consumption. Today's great powers find themselves in a growing conflict over global governance—essentially between a democratic model that endorses the rule of law and an authoritarian alternative driven by power, regime survival, and not rules. In this contest, democratic states should not renounce cyber weapons and their use unless they are suicidal. States must defend themselves and their citizens. If they fail in this central responsibility, their place will ultimately be taken not by some amorphous group of civil society actors or corporations but by another set of leaders or, in the worst case, another, more aggressive State.

The argument for private sector role cannot be based on the assertion that since the private sector owns and operates 80 or 90 percent of the networks, it bears special responsibility. This dubious statistic is immaterial to the use of force and originally came from lobbyists who argued against internet regulation. In 1914, the private sector owned 80 or 90 percent of the ships afloat but did argue for a role in naval warfare. A few private vessels were armed and made combatants, but they invariably lost any engagement with a proper warship, a

James Lewis is a Senior Vice President at CSIS and has authored numerous publications while at CSIS on cybersecurity and how technology is reshaping politics, economies, and security. Before joining CSIS, he worked as a diplomat and a member of the Senior Executive Service. Lewis was the Rapporteur for the UN's 2010, 2013, and 2015 Group of Government Experts on Information Security. He is frequently quoted in the media, has testified numerous times before Congress, and received his Ph.D. from the University of Chicago.

precedent that advocates for private hack-back may wish to consider as they engage the FSB, PLA, or IRGC. Nor were private ship owners invited to the post-War conferences held to reach an agreement to reduce naval armaments and end ship-building arms races. Some argue that since companies operate the networks over which attacks are transmitted, their voices should be heard. Their voices should be heard but in a supporting role. The lesson here is that being a victim does not justify or guarantee a seat at the negotiating table. Entree is provided only based on the cards one brings to the game, and for great power competition, this requires more than cyber-attack capabilities.

Today's tech giants have an array of software tools and could build and use offensive weapons if they chose to violate the law. This leads some to argue that they deserve a seat at the negotiating table since they could engage in conflict. The same could be argued for Russian organized crime, but the Russian state would not permit this. In any case, there is a ceiling on the private potential for offense since companies lack the full scope of military and intelligence assets and are more vulnerable to coercion, particularly from China.

An equally important limitation is the status of private actors under international law, which would make retaliatory action by them a crime, not self-defense. While the authority of states has been diluted in many areas, this is not the case for the use of force and possession of the capability for organized violence at scale, where states still have a monopoly.

Increasing Conflict Constrains Negotiations

The role of the private sector is also shaped by increased inter-state conflict. The international environment is increasingly unstable, and the direction of international affairs is towards greater conflict. It is no longer safe to discount the possibility of armed conflict between major powers, even if these conflicts might be limited in duration and scope. The increased level of international dispute means that cyberspace is a contested domain, where opponents maneuver to position themselves for advantage now and in the event of a conflict.

The absence of overt, formal conflict and the interconnections created by globalization makes it easy to ignore how the international environment has changed. Nations are already in deep conflict, even if it is not the kind of wars declared in 1914 or 1939. Today's conflicts usually involve non-military modes of competition (at least so far). The laws of war were designed for the last century and are difficult to apply to current conflict, chiefly in that the old distinction between espionage and warfare no longer makes sense. The reluctance to admit that nations are in an unavoidable fight is not unusual for democracies. When Ford set sail for Europe or the students at Oxford University declared in 1933, they would never fight a war. Unfortunately, in both cases, authoritarian opponents were not similarly dissuaded.

That said, the future of war, at least among major powers, will try to avoid direct conventional conflict. Wars between big, heavily armed states are expensive and risky, particularly if they involve nuclear weapons. Big countries will not renounce war—Russia, the US, and China frequently use force or the threat of force—but they will try to avoid open warfare with each other. Opponents will exploit the grey areas in international law and practice inflicting damage without triggering armed conflict. If big countries do stumble into war, cyber-attacks will be a part of the fighting, but cyber operations are not waiting for the outbreak of armed conflict. Cyber operations are a new way to exercise national power without stumbling into conventional conflict. They are ideal for the new strategic environment. How countries will use cyber operations is determined by their larger interests, their risk tolerance, and by their existing strategies, experience, and institutions.

Changes in how nations use force or its alternatives complicate the agenda for negotiation because demarcations between peace and war, or civilian and combatant, are no longer clear. One reason for an increased civil society and private sector role is that the Internet has reshaped public expectations for openness and transparency in democracies. This blurring contributes to the question of who speaks appropriately for the actors in a cyber conflict. For democracies, the use of cyber operations is shaped by public perceptions (among citizens, civil society, and other private actors) of the rationale for action, particularly coercive action. Private sector and civil society involvement have become essential for legitimacy, making cyber negotiation no longer solely the domain of states. It would be unthinkable for western nations not to involve the private sector somehow, which does unavoidably complicate the task of western negotiators.

However, the underlying lesson is that actions needed to gain domestic political support do not guarantee international effect. Agreements that lack commitments from the most powerful states or fly in the face of strategic necessity are of limited value, even if private sector actors support them. The 1907 Hague Convention included a prohibition against bombarding undefended civilian targets and was amended in the 1920s (Article XXIV) to similarly restrict the use of aerial bombardment. Another unfortunate precedent is the Kellogg-Briand Pact of 1929, where states agreed not to engage in war (also signed in Paris). At the start of the Second World War, President Roosevelt appealed to belligerents on September 1, 1939, to only use air attacks against military targets and observe their Hague Convention commitments not to attack civilian populations in undefended cities. Britain, France, and Germany quickly agreed to this, but their commitments collapsed (immediately for authoritarian Germany) in the face of military necessity.

Similarly, civil society recently led a successful effort to draft a UN Convention banning nuclear weapons, but no nuclear power has signed it, and the behavior of the nuclear state is unaffected. These examples suggest that while symbolic agreements may serve useful political purposes within the western community, they are inadequate at constraining the use of force. It is telling that the Paris Accord was unable to attract support from members of the authoritarian group of states, suggesting a profound disinterest in a multistakeholder approach to cybersecurity negotiations.

Most cyber incidents fall into the categories of crime and violations of national sovereignty. They are not an “act of war” (a rhetorical term rather than a legal threshold) and do not involve the use of force as it is traditionally defined. The most damaging cyber incidents are actions by states as part of some larger interstate conflict. We will only see physical destruction and casualties from cyber operations when they are part of some larger armed conflict. Such conflicts will involve a combination of weapons—cyber actions will be only one tool. The low-level cyber actions that we have seen to date have a corrosive effect and can be destabilizing, but we do not want to mistake them for warfare and its high level of violence and destruction (a measurable difference). This is important because, in the absence of the risk of significant damage that armed conflict brings, there is little incentive for states with offensive cyber capabilities to make concessions in their use, much less agree to disarm.

The Value of Norms

Powerful states will not any time soon accept a "Cyber Geneva Convention," the binding convention governing cyber conflict sought by private actors. The groundwork of common understandings has not been laid, and these common understandings usually grow from a shared experience of a conflict that both sides wish to avoid repeating. Both the Geneva Convention (and its protocols) and the Hague Convention that preceded it followed violent wars. These agreements were reactive, driven by the experience of warfare. But, despite the standard exaggeration of the risk and effect of cyber-attack, there has been no cyberwar: no deaths, no causalities, minimal destruction. The serious moral imperative which is created by violence and can lead to agreement on restraint is lacking. Those who wield the most power in cyberspace when it comes to offensive action are not ready to agree to stop. This means that the efforts to create cyber peace are, at best, a rehearsal for negotiation and, at worst, a distraction.

Global agreement in 2021 on a framework of responsible state behavior was a significant step forward for building international cybersecurity in a stable, rules-based environment. Still, experience has shown that agreement on norms by itself is not enough to achieve the desired outcome. While there has been a debate over the usefulness of creating a framework of rules for cyber conflict if all do not observe them, most scholars and western government practitioners agree that these frameworks are still worthwhile for cyber conflict. Their usefulness arises not only because a framework of rules exists and some combatant powers have agreed to observe them, but it is also that they provide a justification for counteraction against those who do not observe them. This may be the most important contribution of norms at this time. For norms to have an effect, there must be consequences for nations who choose not to observe them.

Consequences mean the range of internationally lawful responses available to states who are the victim or target of malicious actions that run counter to agreed norms. While there has been some progress towards the imposition of consequences (such as sanctions by the EU or indictments by the US), this has been an ad hoc and disjointed process. Even like-minded nations have yet to develop common views on the full range of internationally lawful responses to malicious actions that run counter to agreed norms, on how to anchor them in a rules-based approach to international order, and on how to harness broader global support.

The successful conclusion of the United Nations Open-Ended Working Group (OEWG) opened many avenues for future work in international cooperation in cybersecurity. One of the most important is that the OEWG reinforced the global applicability of existing international law and the norms developed by the 2015 UN Group of Government Experts (GGE), which, together with confidence-building measures and capacity building, consolidated an initial framework for responsible state behavior in cyberspace. This success highlights the question of how states observe 2015 norms. Some of this involves capacity building so that states have the ability to implement norms in their national policies and actions, but it primarily entails a discussion of what the consequences should be when norms are not observed.

This is not a new issue. In September 2019, 28 like-minded nations issued a Joint Statement at the UN on advancing responsible state behavior in cyberspace. These countries agreed to "work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law." Norms and international law are essential to this discussion of consequences. Ultimately, the agreed norms can reinforce international law to reduce cyber conflict. In the interim, however, it would be useful to consider both a menu of voluntary actions to hold states accountable and the issues that accountability unavoidably raises. These include evidentiary standards, attribution, and information-sharing; mechanisms for coordination of collective action; the relation to other measures, such as the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (or so-called EU Cyber Diplomacy Toolbox); harmonization with international law and the implications of other treaty obligations for collective self-defense.

The status of international negotiations on cybersecurity remains slow, far outpaced by the development of offensive techniques. There has been agreement on initial confidence-building measures (CBMs) in the Organization for Security Cooperation in Europe (OSCE) and some limited progress on CBMs in the ASEAN Regional Forum and the Organization of American States (OAS). In the UN, we are entering the seventeenth year of negotiation on cybersecurity. There has been the endorsement of general norms, the most important of which embed cyber-attack in the existing framework of international law, including the law of armed conflict. However, there is no agreement to end or constrain the use of cyber-attacks in wartime. Nor is there any agreement on the definition of a "cyber weapon" or what would qualify as the use of force or armed attack in cyberspace. This is unlikely to change, and these areas of disagreement limit the applicability of existing understandings on how to govern armed conflict and make it more difficult to create new ones.

Cyber diplomacy, private or not, raises several questions, including whether it is even useful at this time to pursue negotiations with opponents. So far, there is no indication that there is much room for any negotiated agreement. It may help to differentiate the role of private actors in international cybersecurity. However, while their involvement is politically essential within the community of democracies, the as yet unlearned lesson is that it is not essential in, nor effective for, negotiations between democracies and authoritarian states. The role of private actors in cybersecurity negotiations depends very much on the changed context for internet politics. In the 1990s, when the world seemed to be moving towards consensus on governance and conflict seemed to be in decline, a multistakeholders approach made sense. This is no longer the case in this increasingly conflictual international environment, where authoritarians prefer sovereign counterparts and dismiss or downplay private actors. We should adjust our expectations accordingly.

Power Versus Pragmatism: Unlearned Lessons in Dealing with China

Nigel Inkster

The prevailing China trope in Washington is that US engagement with China has been a failure. The argument goes that far from turning China into a status quo power aligned with western interests and values, engagement has provided the Chinese Communist Party with the wherewithal to promote an illiberal agenda that poses an existential challenge to the US-led international order.

This is both true and an oversimplification that masks the lessons about China unlearned as yet by most Western leaders. It is true in the sense that China has in the past decade taken a markedly illiberal turn and is now demanding that the international order should be modified to accommodate its emergence as a major global power. But it is an oversimplification in that US expectations were at least initially more realistic about what engagement might produce. Any review of past official US pronouncements on the rationale for engagement with China makes it abundantly clear that this was never about promotion of democracy or regime change. Rather the hope was that engagement would result in a China that would play a constructive and stabilising role in world affairs, in contrast to the highly disruptive role it had played in the Mao era, and evolve towards an "autocracy-lite" regime. The US government's China experts were under few illusions about the nature of a regime that had demonstrated in June 1989 how far it was prepared to go to maintain its hold on power. Meanwhile China's Party-state had made no secret that the main aim of China's by-then dramatic economic development was to strengthen the Party's hold on power, a reality that western policy-makers chose to ignore.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Nigel Inkster CMG has been Senior Advisor to the International Institute for Strategic Studies (IISS) since June 2017. Prior to that he worked full time at IISS from 2007 first as Director for Transnational Threats and Political Risk then as Director for Future Conflict and Cyber Security. In the latter capacity he was involved in para-diplomatic dialogues on cybersecurity and military cyber stability with China and Russia. He also served from 2017 to 2019 as a Commissioner on the Global Commission on the Stability of Cyberspace.

Prior to joining IISS he served for thirty-one years in the British Secret Intelligence Service. From 2004 to 2006 he was Assistant Chief and Director for Operations and Intelligence.

His publications include *China's Cyber Power, Routledge for IISS (2016) and The Great Decoupling: China, America and the Struggle for Technological Supremacy, Hurst (2020).*

For a long period, engagement appeared to be delivering the hoped-for results. For the better part of thirty years, Chinese society underwent a process of progressive normalisation. The government got out of people's lives and built modern institutions and processes that increasingly operated in a predictable fashion. China went from being a totally closed to a relatively open society. Western businesses were able to operate profitably, albeit in a still somewhat anarchic environment. Moreover, internationally China was happy to behave as a status quo power and to free-ride on US-supplied security goods. But the strategy always entailed risk. President Richard Nixon, the initiator of rapprochement with China, reflected at the end of his life on whether he had inadvertently created a Frankenstein's monster. In 2012 Henry Kissinger, the architect of this rapprochement, wrote that evidence from Chinese official pronouncements increasingly pointed towards a future of confrontation rather than cooperation.

But it cannot be denied that access to western technologies and in particular Information and Communications Technologies (ICTs) gave rise to a China that, as its power increased, evolved into the strategic competitor it has now become in ways that leave the West feeling increasingly vulnerable and disadvantaged. That this came as an unwelcome surprise was arguably the product of a lack of cultural and historical context and a failure of imagination rather than a lack of knowledge; that is to say the lessons were there but not absorbed. As has so often proved to be the case, what has generally been good intelligence coverage of China provided the sum of the parts but failed adequately to convey the whole. An "end of history" mindset prevented Western thinkers and policy-makers from conceiving of how an ancient and very distinctive civilisation might look differently at issues and values that seemed beyond challenge. Nor could they appreciate that such a civilisation might prove adept at identifying western vulnerabilities and exploiting them for their own advantage. This mindset was a major block to perceiving emerging reality accurately and proved enormously consequential as it enabled China to turn western dominance of ICTs into a significant vulnerability. At the same time, it enabled China's regime both to reinforce its hold on power and to shape an international climate more favourable to its interests.

When China first adopted the Internet, it was believed that the free flow of ideas would prove terminal for autocracy. Instead, China showed the world that it was possible to control the free flow of ideas, albeit at considerable cost—it has been estimated that China spends close to $7 billion a year on Internet censorship,[1] a sum which is only a small fraction of the total annual expenditure on China's techno-security state. And when China launched a pervasive and promiscuous campaign of industrial cyber espionage, many of the US corporations who were targeted persuaded themselves that the resultant loss of IP would cause limited damage because China would not be able to use it as a basis for genuine innovation, while US corporations would continue to innovate. Thus, as in Xeno's paradox, the Chinese Achilles would never overtake the US tortoise. And even if corporations were tempted to take action, they generally opted not to do so for fear that Chinese retaliation would result in a loss of market access. Hence, once the US government had begun to assemble a case against China, corporations were unhelpful, and it proved hard to gather evidence.

Both government and the private sector were also slow to appreciate how data would change perceptions of intelligence and of what categories of information needed protecting. In contrast, China was quick to recognise how the collection of large volumes of data that, taken in isolation would be viewed as either unclassified or of low classification, could, when looked at in aggregate, confer significant intelligence advantage, a product of a mindset that took a much wider and more all-encompassing approach to national security than is typically true of western liberal democracies. It has been estimated that 80% of US nationals have had their data stolen by China.[2] This includes financial, healthcare and travel data. Meanwhile, the data of 22.5 million federal government employees was stolen from a federal database that was known to have poor cyber defences. These data sets are now being subject to bulk analysis by China's private sector companies who don't particularly want to do this work on behalf of the state but are given no choice in the matter. Apart from conferring on China obvious counter-intelligence and intelligence targeting benefits, this data has the potential to confer advantages in areas that include economic competition, political interference and possibly, using medical data and DNA, to conduct research into bio-weapons designed to target specific ethnic groups—though there is currently no evidence that such research is in progress or even if this is a practical proposition.

In the US and, more generally, the West, the pendulum has swung from complacency to panic—at least in government circles where China has now become The Sum of All Fears. That panic is arguably overdone. Moreover, it risks giving rise to a classic security dilemma in which US actions designed to protect its own technology interests are perceived by China as hostile and reinforce a mindset that seeks both to reduce reliance on US technology and strive for global technology dominance. But it is nonetheless clear that the US is less well-placed than it needs to be to deal with a powerful strategic competitor mobilised on an all-of-nation basis to achieve some clearly defined strategic objectives. Nowhere is this truer than in relation to many US technology corporations which have evolved into transnational behemoths increasingly untethered from the jurisdiction in which they are incorporated and certainly not instinctively disposed to do the US government's bidding.

The complexity of globalised technology supply chains has meant that it is hard for either government or the private sector to develop mutually reinforcing approaches to China. The intensity of US criticism of China's surveillance state, particularly in relation to Xinjiang, which has served as a giant test-bed for many of the relevant technologies, is undermined by the fact that US technology companies have provided much of the technology that enables this surveillance state. US technology companies such as Qualcomm chafe under sales embargos of microchips to China which account for a significant portion of their global revenues. Paradoxically such sales embargoes may militate against the US' ability to maintain an innovative edge if they translate into less revenue to devote to R&D and a diminished tax base.

LEARNING TO DEAL WITH CHINA AS IT IS

Any effective response to the China technology challenge has to start with the assumption that China in its current form is here to stay and that US efforts to undermine the regime are based on flawed assumptions and certain to be counter-productive. Western experts on China, who ought to know better, have a propensity to batten onto particularly high-profile instances of dissent to make the case that Xi Jinping is deeply unpopular and has many enemies just waiting for an opportunity to unseat him. Examples of this include recent essays by Xu Zhangrun, former Professor of Jurisprudence at Tsinghua University, which set out in forceful but elegant prose his many reservations about the regime.[3] And the YouTube video released in late 2020 by Cai Xai, a former professor at the Party School which decried the Chinese Communist Party as a gangster regime.[4] These expressions of dissent do undoubtedly resonate with members of the educated urban elite. But such views are unrepresentative of the wider population which, broadly speaking, is proud of China's achievements and is quick to rally round the flag particularly when they see China as under attack from the US.

It is also true that Xi Jinping has made enemies in the elite through his anti-corruption campaign, with outside commentators focusing in particular on former CCP General Secretary Jiang Zemin. There is no doubt that Chinese leadership politics are fraught with factional infighting and the anti-corruption campaign has produced losers. It is also true that key poles of power, notably the PLA and the security ministries, have not always been fully receptive to direction from the central leadership. But Xi Jinping either has or is in the process of taking firm control over these constituencies. And, more importantly, everything Xi is currently doing is precisely what he was appointed by his peers to do, namely clear away entrenched interest groups standing in the way of economic progress and re-establish discipline and conviction in a Party apparatus that had been infected by levels of corruption that could no longer safely be ignored.

In Chinese leadership politics anything is possible as evidenced by the dramatic events of 2013 that led to the downfall of former Chongqing Party Secretary Bo Xilai. But there is no evidence that Xi is vulnerable to challenge. And even if he were to be replaced there is no guarantee that whoever replaced him would be either less authoritarian or better disposed towards the US. There have periodically been those within the top Party elite who have sought to promote an image of relative liberality. But experience suggests that even if this is genuine—though it is often no more than a means of differentiating themselves from competitors—the imperatives of maintaining tight social control quickly overcome any liberalising impulses. When Xi was first appointed, many foreign commentators speculated that he was a liberaliser, an illusion of which they were quickly disabused.

LEARNING TO LIVE WITH CHINESE TECHNOLOGY

Determining how advanced China’s technology is relative to that of the US is hard to do, not least because China tends to oscillate between bouts of techno-exuberance and more sober assessments. The latter view is exemplified by a 2020 lecture by Liu Yadong, Chief Editor of the Science and Technology Daily in which he pointed out that China had never developed a scientific culture, as opposed to an engineering one.[5] However, it is safe to generalise that China, though still relatively weak in foundational science, is strong in terms of its ability to develop innovative applications of existing technologies. The Chinese Party-state is also devoting substantial resources to the pursuit of its declared objective of being a global technology leader by 2035. It remains to be seen how effective this top-down push will prove to be, given the impossibility of predicting how some technologies will evolve. Furthermore, it is certain that this approach will result in considerable waste, as has happened with the collapse of projects to develop indigenous production of advanced micro-processors and a variety of projects involving Artificial Intelligence, which were often initiated by entrepreneurs with no relevant technology backgrounds. But the Party can be relied on unceremoniously to bury such failures, learn from them, and move on.

The only sensible course is to recognise that Chinese technology is here to stay and Western states cannot hope to cut themselves off from it entirely. In the same vein, Western states will have to confront the fact that, at some point, China has and will produce technologies superior to those developed in the West. For instance, during the COVID-19 pandemic, the Centers for Disease Control and Prevention (CDC) wasted months trying and failing to develop a test to detect coronavirus rather than using an already developed Chinese test that was demonstrably fit for purpose. And although Huawei’s 5G networks are derived from and continue to depend on US technology, the fact remains that Huawei has established itself as a global industry leader in the roll-out of 5G networks. It is noteworthy that the CEO of one of Huawei’s main 5G competitors, Ericsson, spent much of 2020 lobbying the Swedish government to not exclude Huawei from Sweden's 5G network for fear that any such exclusion might adversely affect Ericsson's China business, including its access to Chinese-manufactured components for its own 5G systems. Such is the level of technology entanglement that has arisen as a result of complex globalised supply chains in which China is often a single point of failure.

In fact Western technology companies have already begun to move some of their manufacturing out of China. This has been driven by rising costs, a less welcoming environment and an awareness of the need to build resiliency into supply networks that have been optimised for efficiency. In this context, calls by the former Trump administration for US companies to repatriate some manufacture to the US, though seemingly driven by mercantilist considerations, may still make sense. The consequences of outsourcing so much of the US' manufacturing are a progressive loss of valuable skills and hands-on experience, neither of which are easily replaced, and vulnerability to supply choke-points. Advanced micro-processors are an example as their high costs have driven most US technology companies to "go fabless" and outsource manufacture to two key locations, Taiwan and South Korea, both of which are exposed to high levels of geo-political risk. The race is now on to repatriate some of this manufacture to the US with the Taiwan Semiconductor Manufacturing Company committed to opening a foundry in Arizona in 2024 that will produce microprocessors at the 5-nanometre production node, by which time Taiwan will be operating at the 3-nanometre production node.

The harsh realities of geo-political competition are driving the US and China apart to the point that some level of economic and technologic decoupling is likely to happen. Now the question is how far that process might go and whether it can be done without irreparable strategic damage. Some within Silicon Valley have begun to look beyond the quarterly returns and to think about China from this more strategic perspective. The China Strategy Group was formed with the aim of considering the most difficult problems of US and China technology competition. Eric Schmidt, its leader, observed in a January 2021 report that:

> America's technological leadership is fundamental to its security, prosperity, and democratic way of life. But this vital advantage is now at risk, with China surging to overtake the US in critical areas. Urgent policy solutions are needed to renew American competitiveness and sustain critical US technological advantages .... as we seek to avoid unnecessary and counterproductive levels of separation, we should also recognise that some that some degree of disentangling is inevitable and preferable. In fact, trends in both countries – and many of the tools at our disposal-inherently and necessarily push toward some kind of bifurcation.[6]

A similar approach has been recommended in a separate report co-authored by former Congressman Charles Boustany and Professor Aaron Friedberg entitled "Partial Disengagement."[7] Both reports argue that the key to continued US technology leadership lies within: developing the US' human capital and making the US a welcoming destination for global talent. Both reports argue that the Federal government should invest more in foundational science and promote greater collaboration between government and private sector, with the intent of ensuring that promising start-ups in areas such as AI and quantum computing can stay afloat until such time as they can commercialise their research. Both reports accept that Chinese technology cannot and should not be totally excluded from US markets and argue for a risk-based approach driven by national security considerations.

Neither of these reports directly addresses the issue of technology embargoes. A decision by the Trump administration to deny China access to the most advanced microprocessors has convinced Beijing that the US will do everything in its power to prevent China from taking its legitimate place on the world stage and has spurred a massive effort to promote indigenous production of these critical inputs. It has also exacerbated US-China tensions over Taiwan, which accounts for 55% of the world's most advanced microchips. The US has also sought to impose an embargo by its allies on the use of Huawei equipment in 5G networks, overriding arguments by countries such as the UK that limited use of such equipment at the edge of the network represents a manageable risk – a position with which US government technology experts in NSA concurred. Such embargoes may serve a tactical purpose in buying the US time to make up lost ground. But it is questionable whether this represents a sustainable approach in the long-term particularly in the event that China does succeed in out-innovating the US.

WORKING WITH ALLIES AND PARTNERS II. NEW STRATEGIC PARAMETERS

The Biden administration has placed great emphasis on the importance of working with allies and partners to manage the China challenge in contrast to the Trump administration's approach, which showed no interest in such relationships and treated allies and partners alike with disdain. This approach scarred the US' relationships, even with its closest Five-Eyes allies. That said, the Trump administration's strategy for the Indo-Pacific, declassified in 2020,[8] suggests that the Trump administration did in fact have a coherent alliance-based strategy for the military aspect of US-China relations. In essence, Trump's strategy amounts to the creation of a lattice of relationships with varying degrees of formality and commitment. Arguably, this approach needs to be extended to cover the full range of issues where China presents a challenge, based on an acceptance that not all participants will entirely share US attitudes or be willing to confront China in the way that only the US has the capacity to do. It also requires an acceptance that the US can no longer take for granted the leadership role it has previously exercised and will be dealing with partners who are, to varying degrees, inclined to strike a pragmatic balance between the US and China if not to play one off against the other. The geometry of the future will be variable. The lesson to be learned is clear. Power will have to yield to pragmatism.

NOTES

1. https://cset.georgetown.edu/article/buying-silence-the-price-of-internet-censorship-in-china/.
2. https://www.infosecurity-magazine.com/news/china-steals-personal-data-of-80/.
3. For high-quality translations of Xu's essays see China Heritage: the Xu Zhangrun Archive http://chinaheritage.net/xu-zhangrun-%E8%A8%B1%E7%AB%A0%E6%BD%A/.
4. https://www.youtube.com/watch?v=EkZ6-YGbwYw (Chinese only).
5. https://www.youtube.com/watch?v=QLON2sFb7qY Chinese only
6. https://petworld-online.com/asymmetric-competition-china-strategy-group
7. Partial Disengagement: A New US Strategy for Economic Competition with China, Charles W. Boustany Jr. and Aaron L. Friedberg, The National Bureau of Asian Research Special Report #82, November 2019. https://www.nbr.org/wp-content/uploads/pdfs/publications/sr82_china-task-force-report-final.pdf.
8. Trump's Top-Secret Indo-Pacific Strategy is Now Declassified, Rory Metcalf, The National Interest, 17 January 2021.

Unlearned Lessons Behind Building a Shared Cyber Framework

with your Geo-Political Adversaries – the Hacker Perspective

Chris Spirito

Even in times of seemingly intractable geo-political conflict, geo-political competitors can find opportunities to develop a common cyber framework – the "Shared Cyber Framework." Achieving cyber stability between two or more nations is not predicated on congruence across all domains of cyber engagement, nor can silence among adversaries advance international stability. From a hacker perspective, this observation seems obvious. Indeed, the technical exchanges during the Cold War between the United States (US) and the former Soviet Union are said to have measurably contributed to both the stability of the bipolar world and, ultimately, the end of the conflict.[1] Yet the current generation of leaders in the major cyber powers have neglected this lesson, both those who exploit access to westernized technologies and those who have responded by attempting to freeze out the attacking nation. For the past few years, the US and China, for example, have increasingly withdrawn from fruitful bilateral discussions. The January 2021 revelations of the Chinese Hafnium Zero Day hack riding shotgun after the December 2020 Russian SolarWinds campaign discoveries suggest few major cyber powers have progressed in finding even small areas of agreement on which to build confidence and a common framework.

Without the lessons that can be learned from common efforts, building spaces in which other areas of contention can be worked to improve stability and peace will be quite difficult. In the hacker community, there is very little trust and yet groups find ways to collaborate in exploits, campaigns, and even distribution of rewards. Using primarily

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Chris Spirito is a Nuclear Cyber Security Analyst for Idaho National Laboratory (INL). He supports Nuclear-Cyber work programs with US partners and is PI for a research program on remote and autonomous operations for advanced reactors. Prior to joining INL, Chris was the International Cyber Lead for The MITRE Corporation. He is also a board member for WiRED International, a global health NGO providing medical education to underserved regions of the world.

Title: Nuclear Cyber Security Analyst

Affiliation: Idaho National Laboratory

Academic Background: Boston College, Harvard School of Public Health, Worcester Polytechnic Institute

the author's experiences in cross-adversary efforts to secure nuclear power plants from cyber-attacks, the following essay identifies axioms for collectively advancing ideas for cooperation, despite wider state-state distrust, and for creating from the bottom up a Shared Cyber Framework.

Find a common problem to work on together in safe domains

When the problem space includes the whole gamut of geo-political conflict, one should avoid domains where the equity dynamics are too fluid to control. What might be common interests in the military and intelligence problem spaces can be immediately excluded, along with international monetary systems and, apparently, pandemic response. Each of these domains is deeply affected by cyber-security architectural dependencies as well as cyber-defensive mechanisms used as a response to hostile actions. Learning the lesson means identifying a domain where both (all) parties are invested in operational success and overtly agree that operational failures would be destabilizing, at a minimum, to their own society, and possibly more broadly destabilizing to the global community and earth's ecosystem.

For example, one area of common interest for geo-political adversaries would be the safe operation of nuclear power plants and research reactors. The horrific impact from a dirty bomb created using stolen nuclear material, or a core meltdown within a nuclear reactor, is almost universally recognized and thus provides a pathway for major powers' engagement. One advantage of this problem space is that, at least in this case, the problems and solutions are not limited to the geo-political rivals, as they extend to all nuclear regimes, and thus there exist engagement pathways with the possibility of many trusted intermediaries.[2]

Leave nationalist ideology at the door

Ideology influences international relations throughout history. Diplomatic relations are shaped by these ideologies, but often these perceptions and judgments instantiated by diplomats become roadblocks to cooperation. Using a bottom-up approach, engineers, scientists, and field technicians can more easily leave their ideology outside the door, and more readily identify their technically trained counterparts able to focus on the common problem and use that joint effort as a platform for confidence building. This advantage was particularly evident during the Cold War technical exchanges.[3]

It does require considerable dissociation at times to rationalize working with citizens of nations whose leadership engages in less than savory actions from targeted assassinations of their citizens to destabilizing critical infrastructure of neighbors due to perceived injury over fallen statues. However, the bottom-up approach allows for targeted engagement[4] and narrow problem-bounded confidence building with the goal of deceasing risk in the problem space and offers an alternative and usable channel for crisis management and de-escalation in the face of cyber campaigns. This approach also allows the diplomatic engagement tied to the technological exchanges to avoid fractious ideological space since, in most instances, mild norms-violating behavior by engineers and scientists can be disavowed from above.

Create a reciprocal immersive cultural exchange

Once a team is in place, invest in reciprocal immersive cultural exchange with the goals of creating deeper emotional connections between counterparts and improving analytical conclusions that seek to represent counterpart positions. Decision paralysis or less-than-optimal engagement pathways are often the result of misreading both event interpretation and reaction options. This is also a cycle that feeds on itself and requires a special type of lateral thinking and ideological mushiness. Examples of this would be the Soviet submariner Vasili Arkhipov, who is credited with preventing a nuclear strike during the Cuban Missile Crisis (strategic lateral thinking) and more broadly, misperceptions by every country that the US is a streamlined bureaucracy adept at centralized planning and coordination. We need this immersive cultural exchange to provide environmental perspective and develop an intimacy with our counterparts to better see the world through their eyes.

> It is intimacy that is supposed to give us a glimpse of different points of view – we might not become the people we study, but by living, thinking, and feeling close to them we should be able to understand how they see the world.[6]

These types of cultural exchanges are not difficult for those open to the experience. In the US these activities have taken the form of foreign technical teams visiting gun ranges and National Parks along with partaking in local culinary treats, such as New Jersey Pork Rolls.

In other countries, as this author has experienced, these cultural exchanges could include more exotic experiences. In the cybered world, critical information about vulnerabilities is not generally shared between organizations; it is shared between people speaking with each other, usually face to face. Requests for assistance in the face of cyber campaign surprises requires trust built on this cross-team intimacy, plus a healthy amount of cognitive dissonance on occasion.

Analyze and Prepare for Political Interference early on

If isolated from wider conflicts, technical team members can focus on solving problems together. The joint focus and associated interpersonal intimacy allow freedom of communication and a generally less bounded information-sharing space. However, the cyber domain is not immune from competing interests. It is important to decide from the outset how team members will handle types of political intrusions. For example, one could be making progress on better protecting a 'Nuclear Reactor Protection System' (RPS) from cyber-attacks and suddenly find oneself being approached in the off-hours with a request that the progress be slowed down. Or, if slowing the results is not possible, then a request for more information on how those new protection mechanisms can be subverted. It is essential to have each team evaluate what equities they will value in efforts to compromise the project, and that they be equipped with analysis and remediation skills. Deconfliction pathways need to be identified and made available in advance.[7]

This requirement is particularly complex and important when counterparts are not citizens of a nation that values free speech and face the possibility that they and their families could face physical harm if they refuse to compromise the project. For example, some signaling options that can established, such as an adaptation of a "warrant canary"[8] to indicate that a partner's freedom of movement and speech have been limited in some way. Reporting political interference through counterintelligence channels may serve as a deterrent as well as leveraging official diplomatic channels to make other parties aware of these destabilizing behaviors. How these actions are authorized and carried out in each country should be documented when identified and shared to maintain a working level of trust that lowers overall risk of disrupted engagement.

Exercise alternative Crisis Management protocols often

There was an elaborate telex connection installed after the Cuban Missile Crisis to link the president of the United States with the party secretary of the Soviet Union so that future crises could be resolved without nuclear exchanges.[9] In 2013 the Moscow-Washington Cyber Hotline was established, and affectionately called the "Red Phone".[10] President Obama used it once to warn Russia about interference in the 2016 election.[11] The difficulty is that such crisis communications devices are used so infrequently that reciprocal exchanges to build trust do not occur. The cyber hotline was established but did not demonstrably allay concerns about preventing a cyber war from breaking out.

In the same way that political intrusions should be prepared for, exercising crisis management channels and protocols is necessary from the outset. One scenario that could be used is discovery of an implant within the shared domain, such as a piece of malware on an RPS, and what the escalation pathways would look like before and after applying this deconfliction channel. This scenario would be exercised from both (all) participants' perspectives, and stakeholders would be included depending upon which de-confliction channels and processes they want to see exercised.

If a bottom-up approach—identifying a common problem to work on, engaging in reciprocal immersive cultural exchanges, and deconflicting political intrusions—is strategically employed from the outset, there is a greater chance that trusted communication channels will exist and can be expanded to include crisis management if necessary. The success of this model also depends upon each participant having developed a commensurate reputation for trustworthiness within their own national infrastructure. To the extent that they are perceived as trusted resources within the crisis management process, their perspectives aid in deconflicting misperceptions and accurately representing response options and the spectrum of counter-responses across states. Increased transparency provided through a trusted channel will help de-escalate responses in a measured way. Furthermore, this determined but incremental approach would also be welcome so that any sensitive incident response processes and procedures can be offered in a gated progression avoiding instability.

CONCLUSION

Today there is no Shared Cyber Framework among the major geo-political adversaries. There does not exist the typical industrial or even hacker group cooperation among cyber domain participants. Thus, the channels that are available in other domains to facilitate crisis de-escalation are at best anemic. The risk of escalation is greater since the rules of crisis management and behavior are not agreed upon and governing relationships among adversary nations as complementary or at least acceptably global competition. To address this challenge, nations need to find a common interest problem to work on together within the cyber domain, and then engage in confidence-building measures such as reciprocal immersive cultural technological exchanges built with the recognition of ideological boundary conditions and how they need to evolve over the course of the relationship. The engagement risk will be contained if the domains chosen for the common problem-solving efforts are not overly contested. The probability of success will likely also be heavily influenced by the individuals chosen by each participating nation and the support provided – especially in avoiding political interference – as the relationship grows. In short, this bottom-up approach so present in the Cold War needs to be a lesson relearned. With patience, measured achievements in shared cybersecurity can be realized.

NOTES

1. Olga Krasnyak, "How US-Soviet Scientific and Technical Exchanges Helped End the Cold War," *American Diplomacy* (2019).
2. Do-Yeon Kim, "Cyber security issues imposed on nuclear power plants," *Annals of Nuclear Energy* 65 (2014).
3. Olga Krasnyak, "The Apollo–Soyuz Test Project: Construction of an Ideal Type of Science Diplomacy," *The Hague Journal of Diplomacy* 13, no. 4 (2018).
4. V. Levitov and H. Long, "US-USSR cooperation in superconducting power transmission," *IEEE Transactions on Magnetics* 15, no. 1 (1979).
5. Jervis, Robert. *Perception and Misperception in International Politics: New Edition.* REV - Revised ed., Princeton University Press, 1976. JSTOR, www.jstor.org/stable/j.ctvc77bx3. Accessed 16 Mar. 2021.
6. Katarina Kušić and Jakub Záhora, Fieldwork, Failure, International Relations, E-International Relations, 2020, https://www.e-ir.info/2020/03/30/fieldwork-failure-international-relations, accessed March 16, 2021.
7. Arian L. Pregenzer, *Learning from the Past and Challenges for the Future: The Role of International Technical Cooperation*, Sandia National Lab (SNL-NM), Albuquerque, NM (2011).
8. Rebecca Wexler, "Warrant canaries and disclosure by design: The real threat to National Security Letter gag orders," *Yale LJF* 124 (2014).
9. Tobias Nanz, "Communication in Crisis. The" Red Phone" and the" Hotline"," *BEHEMOTH-A Journal on Civilisation* 3, no. 2 (2010).
10. Andrew Futter, *What Does Cyber Arms Control Look Like?: Four Principles for Managing Cyber Risk* (European Leadership Network., 2020).
11. Erica D. Borghard and Shawn W. Lonergan, "Confidence building measures for the cyber domain," *Strategic Studies Quarterly* 12, no. 3, (2018).

National Capacity
Unlearned Lessons

Unlearned Lessons: Why They are so Hard to Learn, and What Could Actually Help

Dr. Sandro Gaycken

Cybersecurity is an old problem, and even though many approaches of the last decade had interesting effects, we're still far from solving it. Self-iterative, dark complexity is in the way–an intriguing new plague of our age–and only high talents in the right places with leeway for real-world experiments can rescue us from being outpaced by authoritarian models of innovation. To build that, we will have to break some rules.

Bad old wine in pretentious new bottles

To many newcomers, politicians, investors, think-tankers, and the media, cyber frequently seems to be a dashing new problem, a few years old at best, with high dynamics and many confusing things happening every which way in tech, politics, offense, startups. Many do not know that it actually is as old a problem as digital technology itself, and a static one at that. Initial concerns regarding technology, defense, and politics began in the 70s, increased during the 80s, only to become a rather niche problem in the 90s and 2000s. During these two decades, there were occasional peaks of attention in the information security community, which mainly occupied the minds of nerds, spies, hackers, conspiracy nuts, and a very few companies. In the 2010s, they received some significant attention for almost a decade thanks to Stuxnet, the F-35, and Snowden. This was also when the term "cybersecurity" became more en vogue, much to the amusement of the old information security community who felt sci-fied by it and who frequently still consider anyone using the c-word a noob (google it!). As a side effect, the new term also hid the history of the problem to many. But no: it's not a new problem. The terminology and the attention changed. The problem in all its beauty, with all its structures, causes, effects, and hundreds of publications, had already existed for roughly 50-years.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Dr. Sandro Gaycken is director of the Digital Society Institute Berlin. He published five scientific monographs along with more than 60 other publications. Dr. Gaycken is an Oxford Martin School Fellow, a program committee member of the Harvard-MIT workshop series on cyber norms, a Senior Advisor for the AI Initiative at Harvard Kennedy School, a research director at the Paris Grand Ecole Le CNAM, and an IEEE permanent reviewer. As an advisor to the German government, he helped create Germany's foreign cyber policy strategy and served as an expert witness in NATO cyber counterintelligence cases, and as director in NATO's SPS program for national cyber defense strategies. Dr. Gaycken also founded his own cybersecurity companies. One is SECURE ELEMENTS, now HENSOLDT CYBER GmbH, which applies high assurance computing concepts from DARPA projects to develop unhackable embedded systems for defense purposes. His latest invention is the company Monarch Ltd., a private military intelligence provider with active cyber skills.

That change in the last decade with regards to the public coverage of cybersecurity was dramatic. The persistence of the media attention caused companies and politicians to finally take a closer look and see what the information security community already knew. In the early 2010s, the IT ecosystem was full of vulnerabilities and only gave very little superficial and peripheral attention to security. At the time, there were few effective remedies at hand and growing dependencies, inter- and intra- functionalities exponentially, and increasing with huge potential negative effects of global strategic proportions. It took a few more years before people took this insight seriously, partly because the IT industry feared regulation and negative market impacts, so it stymied conversation around the topic. But since we have all acknowledged that cybersecurity is a real, hard, and a bad problem, much has happened in the past 6 or 7 years. There is now a lot of regulation, constant senior management attention in the corporate and political worlds, large IT companies invest heavily in improving their architectures and removing vulnerabilities. Additionally, IT-security startups draw numerous investments, a flurry of conferences, workshops, and diplomatic efforts erupt annually, where almost every country in the world and every criminal organization want to own and do offensive cyber.

At this point, it would be interesting to take a brief look at COVID-19, which is another big problem. Fortunately, the reality is much less debatable than the need for cybersecurity, although it is also very complex and with a high potential impact on society. The incredibly thrilling element about COVID-19 is how fast we arrived at multiple effective solutions to this problem. From the first lockdown to the first wave of effective vaccinations was one year. Just one year! In contrast, given that cyber is also a high-pressure problem consuming billions in research and development over the past decade, we have not achieved much; nothing in the way of a "vaccine" or any major improvements.

Of course, regulators, the IT industry, and all those IT security vendors will consider this debatable. New laws have effects and more sectors are regulated. More products cover more vectors. So yes, there was a change, and, yes, it did get better. We did get something. A lot, even, measured in pure quantities. There are tons of regulations, many new products, hundreds of new startups, improvements in architectural security in the big IT substrates. But then again, hacking is still possible. It got more expensive, took more time and skill. But you still get access to any system you desire. Believe me, I have the catalog. And the reason for that is that all these flashy improvements have blind spots, functional shortcomings, or other significant downsides, with many entanglements and leading to so many compromises that no real hard security has been built, although it is technically possible. Let us take a more detailed look.

IT regulations are either specific and then outdated when they come into place, or they are unspecific and unintentionally grooming a lemon market where the cheapest product to compliance is the default for most of the regulated (which generates the kindergarten level of security). Many of them are also in conflict with other regulations or economic and political interests, such as data and consumer protection or rolling out new paradigms like smart grids, smart cities, or the Internet of Things. As a result, they are frequently sabotaged and require tedious negotiations during which other political needs and favors are brought into play, watering down potential outcomes. Acknowledgment of a horizontal function and competent senior leadership, a Churchill of cybersecurity, would be required to solve that problem. Still, the regulator's competence is far from sufficient for that, as is the willingness to appoint something like a Churchill in such an embattled field of competing interests.

Almost all critical national infrastructures have some "cybersecurity" now. The bigger, the better, but even the small ones have taken care of some basics in information security. This has increased the overall level of security; not just anyone can enter an infrastructure with pre-configured passwords of the "12345" type anymore. But while teenage kids are now mostly kept at bay, what most infrastructure suppliers are willing to pay and what the market delivers for that kind of money is a different story. The overall level of security is better than a decade ago, but in terms of attack effort, not by much. It is a well-known problem without a good solution at hand, and presumably another decade of painful trial-and-error ahead of it. The list of problems is simply too long: too much old legacy IT, old copy-paste libraries, proprietary protocols, some of which are from companies that no longer exist, high defect rates with old bugs, structural flaws in baseline security features, bad security engineering culture at the suppliers' and operators, tough requirements on uptime while the program crashes much more easily, too many mixed-criticality systems emerging with new networking paradigms, conventional IT-security with its tolerances and technical perspective not being a natural fit, and so on. No wonder there is no one-size-fits-all miracle cybersecurity product on the horizon (although many try to market theirs as one).

So, what about the new products from the hundreds of startups? Can't they offer a remedy, with allegedly so much innovation going on everywhere? Not really. Most of the "new" products don't learn from history and follow old paradigms like "detection" or "incident management," which have nothing but failed us before and will continue to do so. The vast majority of the flashy new technologies, approaches, and companies are in this camp: old (and bad) wine in new (and expensive) bottles. Oh, and not little of that old wine even being snake oil. Snake oil salesmanship is always highly rewarded in cybersecurity.

Makers of products that follow new paradigms and bring real change but have severe difficulties explaining their approaches. It is notoriously difficult to assess the impact new ideas could have on security and the potential conflicts with the function of the technology that it's supposed to protect. Unfortunately, information security resembles natural science in this respect. As the potential interactions are too complex to make accurate predictions, any evaluation requires a high degree of experimentation and trial-and-error, with many critical voices and arguments from science, evaluators, and competitors. As a result, many of these new solutions under scrutiny will turn out to be less effective than assumed, which many of their inventors know upfront. Yet, given that cybersecurity is still a highly competitive market, literally all these new products and startups promise blue skies and green fields. They must if they want to generate any degree of attention in this very noisy marketplace.

As a result, new ideas are not anything investors, corporate businesses, or government clients will jump at with high enthusiasm. In some cases, new ideas may draw enough attention from venture capital investors that they may get an investment. Still, it is much harder to get this kind of money and also much harder to push an entirely new product into the market against less invasive, cheaper, and more well-known products. And, at least in Germany, some venture capital investors tend to have humor failures if their risk is not rewarded, so they sue the founders to get some money back. This is very common here and not a particularly good way to incentivize entrepreneurship. If a new idea is supported by an authority with a sufficient pedigree (say, from MIT), it stands a better chance in the market, but many authorities have already signed up with the big IT companies for more money and are thus required to support whatever paradigm big IT thinks is best for business.

Most of the serious security improvements of the last, more hectic decade of information security can be located within the architectural improvements in the big IT substrates. Here, a lot of progress has actually happened and radiated into the wider hemispheres of the problem. We have a measure of security in this field, which boasts impressive progress - the exploit and implant market in offensive cyber.

The prices of exploits and implants underlie many dynamics such as market demand, export control restrictions or similar political decisions, shortage of real talent, quality, exclusivity, reliability of the vendor, fittingness to particular problems or chains, the openness of clients on issues, trust in general, etc. Additionally, successful operative hacking does not require zero days unless high-value targets are of interest. However, the dynamics in this exotic part of the overall information security market show something very interesting.

Before the last hectic decade, finding and exploiting an access-all-areas, free-beer, total-party zero-day exploit in Windows took about three weeks and was a difficult sell in a black market (a white or grey market did not exist at that time) as too much of that was lying around in the first place. Today, finding and exploiting an exploit for Windows, macOS, or many Linuxes takes six to nine months, and it is most likely far from a total-party exploit, requiring a chain of up to ten or more other exploits to actually get full access. Plus, you require a sophisticated implant to do your bidding inside the system, with many security-evasive measures built-in and very skilled operators with a big fat handbook of dirty tricks to deploy all of that. This improvement is due to the big IT companies paying attention to the problem for several years now and throwing a lot of money at improving their baseline security in architectures. This was a highly effective endeavor - and it is visible in how high prices for exploits have risen. A significant strategic security effect of this entire dynamic is the phenomenon that the low end of cybercrime and state-run hackers cannot simply use the same old methods or zero-days for their activities to go after high-value targets anymore. Many of them got more creative and still get in through social engineering or other silly stuff, but most of them had to settle for lower-end targets and leave the high-end targets to the few high-end attackers. This is one bit of good news from the last decade of improvements.

But is it sufficient? Not really. Even if security in some of these cores improved significantly, attacks still exist, and attackers still get in. Again: I've got the catalog. Why? For once, the big cores are simply too big (and continue to grow faster than they can be tested) to ever be without significant vulnerabilities. Even though prices have soared in the global exploit market, there was never a shortage of supplies. The fantastic, single-hit, access-all-areas backstage pass exploit is much rarer than ever before, almost a mystic beast, one to have back-in-the-old-days drinks over, but if you know how to build a chain, you have some money, baseline competence, and contacts, you will be fine. But even if you do not have that, there are still options. IT is a system with many different components, which will never be from one of the big core IT companies. SolarWinds is an example; and the system, sadly, can still mostly be subverted through its weakest link. Some core assets may still stay secure with new architectures and high assurance secure elements, but a smart attacker will still have enough leeway and options to do whatever they need to do. This is well-known and – sorry – a decades-old supply chain issue. And once attackers are in, they can still scale their attacks every which way and wreak havoc up to a strategic level. We do not see open havoc all too often because (also but not exclusively due to exploit prices) all attackers prefer tactics and strategies which enable them to remain hidden deep inside the system, but for those who know, the option is clearly there, anytime. While individual IT companies may be fine with their reputational concerns and able to blame others and fend off regulation (which is their primary interest in security in the end), the total system security is far from effective. Billions spent and no cyber "vaccine."

Now how can these problems be solved? First, we must acknowledge that cybersecurity is a rather classical case of market failure and a lemon market. Politics would have to step in and regulate. But politics also fail. They're too stupid and too scared to admit it. So, what now? It will help to look at the crux of all levels of market failure from innovation to investment to clients and policy failure alike. I'm a philosopher by training, so I can take the liberty to invent difficult words for key points, and the one that seems to be most fitting in this case is self-iterative dark complexity. Deal with it!

The interesting problem of self-iterative dark complexity

What is it, and how does it apply to cybersecurity? Problems which are (1) highly complex, (2) highly interactive, (3) under constant change or intentional alteration and manipulation with sometimes systemwide effects, (4) epistemically distributed into many different scientific verticals, (5) with many competent actors with biases and competing interests, (6) with many more incompetent actors operating on narratives, biases, paradigms and also with competing interests, and finally (7) with many dark and inaccessible corners, where assumptions, lies and mythical beasts can roam freely, some of which affect fundamentals for the derivation of empirical evaluations – such problems contain self-iterative dark complexity. In these cases, the scientific method fails us in a very specific way; it renders it impossible to collectively build validated knowledge. Since the knowledge system is vertically too complex and consists of too many interactive moving parts and since vertical paradigms are partially based on assumptions about dark corners, there is no solid ground from which to exclude or include hypotheses across verticals (and in many cases also inside verticals) in an empirically verifiable way. Collectively built knowledge cannot spill out of verticals to ever create collective horizontal knowledge across verticals which would be required to make decisions with little uncertainty about impacts.

This seems to be a prevailing problem in many fields of great complexity and with humans involved with interest and impact. Other examples of such fields include financial markets or climate change. But let's take a closer look at cybersecurity from this perspective. How do the individual characteristics of self-iterative dark complexity apply, and what does this imply if anyone would seriously like to solve the problem (assuming we even find someone willing and able)?

First, let us look at the implications of complexity. In the true sense of the term, the most complex element is the IT substrate and options to attack and subvert it through hacking. The limit to how someone can attack and subvert a highly complex, semantic IT system, including elements like design, production, peripheries, supply chain, and naive users, is literally the hacker's creativity. While methods can be categorized along a kill chain or in

MITRE’s fantastic ATT&CK methodology, technical implementations of such methods can vary greatly. New methods can come up whenever someone versed in exploitation finds the time to sit down and play. And since computers are language-based machines, the number of attack options can theoretically be determined by Turing’s Halting problem: it is infinite, as an infinite number of misunderstandings can be generated, many of which may constitute a security issue. In practice, it may be different due to the limits of even the most creative hacker, but at any rate, it is enough to create genuine complexity in offensive action. This already radiates complexity into the entire system, as the problem information security must solve to stop this infinite number of options for attacks. While this may be solvable for certain methods or categories of attacks or (an interesting architectural paradigm for computer security) in finite machines, it will never work entirely in complex Turing machines. In fact, despite computer science being an engineering science, most researchers agree that large parts of it now resemble natural science, where you have to experiment with the machine to find out how it behaves. And the technical complexity, which is growing exponentially and is already far too massive for any given IT expert (ask them while having strong drinks, and they will admit it), is not even the only complexity to consider. The entire market environment, the use cases, the legal and political, the regulatory environment all add complexity, all can add vulnerability, and all of them are already too big to understand by themselves.

Second, the complexity is interactive. Any change in the technical, industrial, regulatory, political, or the use case environment can create rippling effects across the system at large and end up producing new weaknesses in very surprising ways. In the technical plane of the problem, this is a very fundamental issue with many unforeseeable effects. But even outside the technical sphere, a lot of this can happen. A good example is a diffuse regulation, incentivizing companies to buy cheap security products which have more vulnerabilities than the system they are supposed to protect while enjoying high privileges, thus making it easier for attackers to attack a system. Great job, politics.

Third, the self-iterative element comes into play. Information technology is not set in stone. It changes every day in dramatic ways. Each developer globally adds roughly a hundred lines of code per day to the total system, much of that interacting with other technologies. So while certain anchors may exist, such as trusted cores without significant change, the system at large is under constant change. Much of it can potentially impact other parts, which cannot be anticipated as the range of interactions and use cases cannot be anticipated.

Fourth, the complexity is too much for humans to understand. It is epistemically distributed into many different scientific verticals, which individually already consume the full attention and intellectual capability of even the brightest minds. This applies to computer science, where a hardware security expert cannot fully understand or work on operating system security anymore and vice versa. Still, it is even more difficult when a technical expert is supposed to work with a policy expert or an industry expert. In addition, verticals tend to conflate and deepen their world and compete with other verticals on their importance because this is how funding impacts the environment. This competition frequently separates them from each other. It sometimes incentivizes them to accept and reproduce certain simplifying narratives of the problem at large if that helps get the upper hand in the competition. In addition, verticals in this highly complex field rarely produce hard paradigms. Others outside the vertical could derive solid knowledge about it in a horizontal perspective, covering the range of reliable insights of the verticals and deriving action items.

At this point, a brief remark about the role of narratives is important. Whenever a field is highly complex and needs to be translated into layman's terms for practitioners, decision-makers, the public, clients, grandmas, or children, a common practice is to use narratives. Narratives are a short version of causally linked facts with specific opinions derived from them and then connected into key messages, sometimes involving unicorns or fairies of sorts to spice things up a bit. The upside of such narratives is that people who are not deep in the respective facts and fields can participate and form an opinion. The downside of narratives is that they actually do that - while essential facts are not included in the narrative and while the narratives narrated in the best way usually win most of the attention, rendering laypeople into victims of that specific perspective of the narrator. The more complex the field, the more options exist to craft narratives and derive opinions. This is hugely important for the next two elements.

Fifth and sixth, the competition of verticals does not stop at science but continues in politics and industry. Competent and less competent actors engage in discourse on these playing fields, ideally establishing a neutral and honest scientifically informed political and industrial debate to arrive at effective solutions. But since they talk across verticals and with many vertically less informed stakeholders, narratives are required. And at this point, the process of knowledge generation fails us again. There are simply too many actors with bad competence or bias but good storytelling skills capable and willing to hijack relevant discourses.

A great example is the "Paris Call," a massive political protest stemming from different IT industry parts, under the rationale that "they know what they are talking about." The members of the Paris Call have political claims and suggestions for many different aspects of our problem, told in a grandmaster narrative, very understandable and, on the surface, politically-correctish. Macron has gobbled it up, as have many other politicians and state institutions. But the entire show is nothing but a vast pile of IT industry lobby garbage, biased manipulative interest, with half-baked arguments as support. Yet hardly anyone is challenging it. Vertical experts are spread too thin and organized too poorly, many of them have contracts with some of those involved and are not willing to bite the hand that feeds them, and many decision-makers don't want to speak out on something they don't fully understand, even though they suspect something fishy. In France, fortunately, ANSSI, the national authority on cybersecurity, has spoken out against it, as have some others, but with comparatively small voices and no master narratives. This happens all the time. Interested actors create gravity around manipulated narratives, which less competent actors cling on to as it appeals to their level of understanding and as they can hide their lack of competence by slipping under the umbrella of a higher authority with undebatable competence.

The dark element comes into play with the seventh point. Now it gets sexy. In political and scientific discourse, any layperson would suspect that facts can solve this problem of lying and cheating. Except for the dark corners of the netscape are areas that play a crucial role in deriving arguments and are not systematically empirically accessible. The darkest corner and the root of almost all the other dark corners, later on, is the offense. The offense in cybersecurity is such an art and so difficult and complex that almost no one can derive systematic horizontal knowledge about it. It is arcane and highly complex on a technical level in analysis, development, deployment, and operation; it is esoteric and complicated on a human level in actual operations, politics, competencies, economics –and none of it is visible as it is almost always either secret or criminal, so in the shadows either way. The visible part of this iceberg—security testing, hacking conferences, and the occasional leak or detected and analyzed attack—offers only a glimpse into what is happening and mostly one in a rear-mirror of something that is already the past again. And those who are in the know here rarely make it to the other side in defense.

For good hackers, offense is far more profitable, and spies and criminals do not change their field of activities very often, plus they are not allowed to talk details about their previous activities. But as all military thinkers and common sense alike tell us: offense is the base problem of defense. And if you do not know how offense works (because you only see the biased, different, and less competent tip of the iceberg), you cannot do defense. For most approaches, neither fittingness, effectiveness, nor efficiency can be predicted with precise or sufficient reliability or coverage. These aspects can be post-dated for events from the past and predicted for some narrowly defined categories of attacks, but since the complexity offers so many different, non-linear futures, that does not guarantee for the future, so there cannot be a solid statement about our security. Furthermore, if no one sees the real iceberg, the great narrators can invent all sorts of assumptions about what that looks like to support their interests and present their narratives as principles and facts.

So, this is the problem of self-iterative dark complexity. In sum, it renders the process of generating knowledge relevant to decision-making incredibly hard. The common processes of collective knowledge generation and decision-making simply do not work here. It is too hard to find actual anchors for real progress, in the middle of a storm of biases and interests and missteps.

How to solve the problem?

So, what can be done to solve this problem?

Continuous, expensive, offense-informed, and rapid trial-and-error (in actual reality and not just some research lab) could help as a process. But in addition, and parallel to other problems with self-iterative dark complexity, no one wants to make a wrong decision or have made a wrong decision. So many decision-makers confronted with self-iterative dark complexity tend to do one of three things. First, they do not make a decision at all and hide behind other issues or try to push the decision to someone else. This is such common practice that hackers have an abbreviation for it. It is the "OGP"-strategy. OGP means "Other Guy's Problem." Second, they hide behind authorities such as the big IT companies pushing the Paris Call. In this case, they can always say, "but they did it too, and they must be right." This, in turn, creates gravity for the associated master narratives as the decision-makers who should be neutral and open for trial-and-error now have a vested interest that the authorities they signed up turn out to be right. The third option is to make their own decision, which happens mainly in the more peripheral areas of the problem such as advanced research or startup investments. In this case, however, due to public pressure, high costs, heavy competition, high visibility, and great rewards for success or severe penalties for failures (try to get an investment for a new startup if one has failed), the choice that has been made must have been the right one. So, although this field would be one with great outlooks for trial-and-error, there is little tolerance for the "and-error" part of the process, with any aspects of that being denied as long and as hard as possible.

Another option would be getting better and more neutral competence into knowledge-generation and organizing the translation of that knowledge into decisions. But this is no real news. We have known and admired this problem for a very long time. Raising competent cyber forces or cyber strategists is the most pressing urge of all governments and industries. Funnily enough, I know numerous instances where the government secretly thought that the private sector must have been ahead of them because they could hire real experts, while the private sector secretly believed that the government, with all its might and insights must have much better knowledge about the problem. So each one was eyeing the other and trying to copy them only to repeat their mistakes.

The most beneficial entity to solve the problem of self-iterative dark complexity would be a competent and politically powerful government agency. That would be a game-changer. But cyber capacity-building in governments just does not work either.

Why? Because there is a severe talent shortage and tough competition with the private sector with outrageous salary gaps. Of course, most governments have fabulous cyber experts working for them, who have insights into offense, know a broad range of products and approaches, and could lead a strategic effort to success. Unfortunately, it is rarely more than a handful (very literally!). And a handful is not enough. To address the entire complexity of the problem, you must distinguish lies from facts, and functions require large teams and a collaborative effort with honest support from outside experts, which is just impossible to build. Many of these fabulous experts have changed many things for the better. But it is a drop in the ocean compared to the avalanche of biased and noisy pointless things happening. This problem was also getting worse under recent political attention. Responsible politicians acted responsibly and allocated resources to cybersecurity in government agencies. Much of this went into tech, but much also went into personnel. This, however, turned out to be more of a problem than a solution. Given the ridiculously lower salaries (often factor 10), governments can only hire a low range of talents. But in that area—hundreds of them. Now hundreds of semi-competent cyber people act as described above and pledge allegiance to shortened, biased narratives while building their own little niche inside those. This, however, again creates more issues and, in many cases, only more nonsense instead of empowering those few real high talents in government.

So, by and large, this is a massive problem with wide-reaching effects, but fortunately, it is a problem with a simple solution. Governments must get talented people into their services to support the loyal high talents they already have and eventually find some minor meaningful tasks for the cyber riffraff or fire them. And THIS will actually be a major task for all Western governments in the future because our futures will be more technologized and more complex than they are now and sufficiently large groups of high talents are – at least at present – the only thing that will help.

But how do we get high talents into government service? Simply paying them what would be necessary does not seem to be an option due to the rigidity of government employment rules.

Four other models exist. The first is the model authoritarian countries use. Sadly, it works very well and has solved the problem for them already, creating a rapidly accelerating edge for them in deep tech and high-tech national matters and a strategic erosion of associated capabilities and effects for us. You simply force the high talents to work for you. No startup, no high salary industry career. Government service. Period. Nice and happy government service, so you do not defect. But government service. Period. But that’s not a model for us, of course. What are our options?

The second model is the Israeli one. You incentivize young people to come and support the government in return for a world-class education and options to found your own startup later and become a gazillionaire. This model seems to work reasonably well but has its downsides as well. A funny one just came up recently. The young soldiers, relieved from army service and under investment pressure in their startup, immediately apply what they learned to a product and sell it on the global market within months. However, the army’s innovation curve is just not steep enough to be around the next corner already, so Israel’s enemies simply buy their startup products to reverse engineer them, in turn, finding and denying Israel's operations around the world. This annoying side-effect led the Ministry of Defense to put cyber exploits under conventional arms control, in turn making every sale a painful, months-long process during which most exploits are being patched and turned worthless and (intentionally) ruining this part of Israel's vibrant startup landscape. Many of these talented young Israelis established defense startups but with mediocre success. A few of them are brilliant, but due to the complexity of the issue, defense is simply a different job. I can tell you this from experience: the almost-last person on earth you want to configure your defenses is a hacker (the very last is the CFO). You want a hacker to look at it, definitely, but not to actually code it. Don't do that.

The third model is the revolving door in two variants. Either contractors come in as hires, working for governments on industry salaries, or they come in for a time and go back after a while, supporting the government temporarily and getting some excellent contacts out of it. Again, both options have negative side effects. With contractors being hired into the government, control and oversight mechanisms do not always work; the collateral damage being incidents like Snowden with massive strategic disruptions among allies. The revolving door expert on the other hand will always be on the lookout for the next super-job and will be tainted with pre-fixed loyalty to his next employer (or at least not wanting to bite any hands they may want to work for in some other future).

The last model we know is outsourcing the problem as a tech issue to the private sector. This can either happen as outsourcing to large companies or startups. Large companies, sadly, are mostly nothing but a copy of government agencies. Big, bulky, slow, uninspired, in parts lazy, no place for high talents, cheap, and of course biased towards profitability, not towards security (which are two very different things in a lemon market). Startups would be in the right place to build external expertise and set up a functioning process as they have the high talents. High talents love startups. But here, government procurement is pure cancer. While strategic government levels may decide that startups are important and must be supported, procurement agencies think procurement procedures are important - and take their time unless they are explicitly overruled. And that is a lot of time—to get into a government contract takes 24 to 48 months. Sadly, many newer approaches like the German Cyberagentur fail to bypass that time frame as it is simply a government mentality thing. Even if legal and procedural levers are set "go," the cautious bureaucrat will still go for the maximum of "cover my ass," especially under new circumstances – and rethink, reconsider, be advised, be reconfirmed, etc. For startups, that simply does not work. New companies with high talents and focused on difficult strategic problems easily burn a six-digit amount of Euros per month. Investors only give you up to 3 million Euros at best. Accordingly, startups' probability of compromising into some detour to a lemon market product is very high. Or, in offense, take a little trip to a less ethically troubled country to sell some products for suitcases of cash while proper countries take their time to consider and reconsider their options. Or those startups simply die. It happens a whole lot, burning time and talent, trust, and incentives.

So, none of these options seems to be mature just yet. All of them fail either because of the salary problem or the procurement problem (totalitarianism not being an option).

Thus, the lesson to be learned is simple, short, and sweet and doesn't require much theory or explanation. Look at how short this paragraph is! One of those two sets of rules has to be broken to pieces and written anew. Better both. Suppose our societies want to be equipped for the vastly complex challenges ahead of us, which applies to any problem with self-iterative dark complexity. In that case, they must have high talents understanding those problems in a neutral and democratic way, and high talents actually building technical or economic, or political solutions to these problems. Which, by the way, will also provide us with an instant edge against our totalitarian competitors, as our systems will be more flexible, heterogeneous, and adaptable than theirs. But getting there is super hard, incredibly disruptive, and needs to be executed real fast. Badly needed are entirely new government payment schemes and procurement rules or simply more radical outsourcing of state functions to the private industry. Paying higher six-digit salaries, buying deep tech within a few months, and letting private startups handle the technicalities of complex economic and political issues. Nothing less and nothing much else. Undebatable, by the way. In addition, even then, trial-and-error will be required. Self-iterative dark complexity can never be conquered or entirely solved. It can only be surfed by high competence on waves of real-world trial-and-error experiments. This is what we have to build. Or dinosaurs will rule the techno age. And die out once again.

Fighting Alone is called Losing: The Unlearned Lessons of Fragmented Systems

Lieutenant General (Ret.) Edward Cardon

Cyberspace is a man-made, contested, and competitive domain that is continuously evolving and adapting at speeds and scales difficult to comprehend or imagine. While hardware is geographically located in a physical layer somewhere on earth or in space, the software and data can move freely in a logical layer unless otherwise constrained. The result is a global surface that requires a globally coordinated defense by a global team. Therefore, within the context of cyberspace, the idea of "defending alone" seems ludicrous. Yet, that is exactly how people, firms, and governments have been left alone to approach cybersecurity. As noted in his comments on the SolarWinds hack in March 2021, General Paul Nakasone, the commander of the United States Cyber Command stated that, "[I]t's not that you can't connect the dots. You can't see all the dots. And when defenders *can't see all the dots*, security gaps and breaches happen."[1] Ultimately, the cyber domain's primary lesson is that leaving everyone to defend alone leaves everyone to lose.

Defending in Cyberspace

What makes cyber defense so hard? If we think of the Internet as a neighborhood with associated crime problems, cyber-crime and attacks are quite varied in their approach, intent, and execution. For example, cyber actors use tools and techniques such as malware attacks to break into systems, devices, and networks to steal sensitive data, information, etc. Similarly, cyber actors use social engineering techniques, often referred to as hacking the human, to hack the network. Other cyber actors cut off access to critical services through denial-of-service attacks. Cyber criminals use tools and techniques such as ransomware to deny critical systems, networks, and data. Finally, some cyber actors attack the very structure of our networks and critical systems through hardware or software supply chain attacks.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

[1] https://www.cyberscoop.com/nsa-solarwinds-russia-china-nakasone/

Lieutenant General (Retired) Ed Cardon's service to our Nation spans over 36 years including work in Germany, Bosnia-Herzegovina, Iraq, and the Republic of Korea. He both transformed and scaled U.S. Army Cyber Command into a world-class cyber force with new organizations, operational constructs, and talent models. Since retirement he has created a portfolio focused on helping individuals and teams solve hard problems with Touchstone Futures, C3 AI, The Cohen Group, and the Advanced Research Laboratory for Intelligence and Security.

Cyber actors can attack using a combination of the techniques as discussed above, can develop completely new techniques, or can even use some combination thereof. And cyber actors do not have to be malicious or criminals – they can be activists, nation states, or normal citizens. Even when an intrusion is discovered, it often takes a deep, multi-disciplinary analysis to confirm the intent behind an attack, and often leaves unanswered questions for cybersecurity experts and professionals to ponder as defenses are evaluated and updated. Was it an information assurance problem? Was it an insider threat? Is the attacker a criminal? Was it a nation state? Could it have been a hacktivist?

The complexity is not just from the threat, but it also comes from the domain itself. The cyber domain is made up of an ever-changing confluence of people, technologies, and processes. It is characterized by disruptive technologies and applications. Time is an important component. Software changes at the speed of coding. Hardware changes at the speed of chip evolution and is increasingly becoming software based. People can change the cyber domain at the speed of thought and learning. In many ways, cyberspace remains largely unstructured, especially when considered in the context of a political map, detailing the physical and sovereign boundaries between nation states. Without physical delineations to define jurisdictions, the established law, authorities, regulations, processes, structure, and concepts applied to the cyber domain are still in flux for both the public and private sectors.

Therefore, it makes little sense to ask all network users, providers, and suppliers to defend their networks, data, critical systems, and information alone, and expect success. Even with the very best technology and processes, when combined with all the potential human factors, there are vulnerabilities in every network. It has become increasingly clear that all networks, regardless of location, are in daily contact with a multitude of cyber adversaries and threats. Risk of compromise continues to accelerate past what fragmented defenses can withstand.

Three Components Essential to the Team

The lesson to be learned of cyberspace is that decentralized, uncoordinated, standalone defenses are ineffective, and the solution is to create a team to defend our networks and critical systems. At a minimum, this team should contain at least three components – the *owner* of the network itself and all its suppliers; the *government's or governments'* competent representatives or authorities; and the relevant or affected actors in the *private sector.* These three components include multiple sub-units, making it a *team of teams* with each component playing a critical role to avoid fighting alone.

One challenge is that a network is often mistaken for a single entity vice the sum of various individuals' work hours and hardware vendors e.g., end devices, network devices and peripherals. A network is in reality a complex set of component parts that must be integrated, configured, and administered by the team responsible for building, operating, and sustaining the network, and the owner of a network hires that team. Additional network elements also require management: e.g., an Internet service provider, software vendors for products and services, software applications and services that are available on the network, and all the data generated from network use among all its various components and users. Ultimately, a network is never just a network.

Also, networks are rarely stand alone or operate in isolation. As more operational technology components come to rely on IP-based services (i.e., the Internet), more systems are exposed to global threats. The idea that an in-house network administration team can manage a network – both internally and externally – to protect it from all forms of attack is an unrealistic expectation and has been for some time. For example, a typical network analyst is responsible for evaluating, planning, ordering, and installing any technology required for a network, requiring a knowledge of the network user needs, network data and baseline measures, and other skills that require a deep expertise. Increasingly network data analysis is being transferred to various forms of autonomy, automation, and/or artificial intelligence. In addition, information and intelligence is needed on cyber actors and potential threats e.g., their infrastructures, their exploits, their tactics, techniques, and procedures, etc. The in-house teams (even if they do include third parties) have long needed additional support structures to escape fighting alone.

The government has a role in supporting a collective defense. Unfortunately, a major weakness is the lack of organization in the US (and elsewhere) at all levels (federal, state, and local). As shown by the past decade, the U.S. Government's (USG) approach is often too fixated on physical harm. All lesser forms of harm are consolidated and effectively dismissed as just the cost of doing business. If an ongoing cyber-attack caused obvious and palpable harm in the physical world, the likelihood of government action would increase immensely. This is exactly what happened with the 2021 Colonial Pipeline ransomware attack.[2] People standing in line because gas stations were closing pumps was a physical manifestation of the cyber-attack and many agencies, most publicly the FBI, sprang into action. That was great for the Colonial Pipeline company, but it is not possible for a private company to legally replicate the cyber capabilities of the USG that can take a more proactive, defend-forward posture in cyberspace. To be fair, government responses to cyber-attacks have improved over time, with the creation and redesign of organizations, commands, information-sharing forums, and the revision of statutes and policies, but much work remains to be able to operate defenses at the speed and scale of the various threats.

Part of the team solution is to bring to bear all the components of the private sector that enable the creation, protection and sustainment of networks and associated data. The growth in private sector cybersecurity capabilities has been significant, but advancements tend to maintain an inward focus on protecting internal data, systems, and assets, like intellectual property. Most cybersecurity decisions are driven by the technological innovation expected of these companies in support of their own clients, products, and profit forecasting – not in a manner that will support a collective defense.

Much of the network space and the data needed to understand a cyber-attack are located with and owned by the private sector. There are several legal and/or regulatory issues that limit or prevent the sharing of information between private companies, cybersecurity companies, or governments, primarily over concerns about liability, privacy and civil rights, and reputational risk. And because most of the data that is needed to conduct a holistic and thorough investigation after a cyber-attack is collected, housed, and stored in the private sector, cost quickly becomes a factor that determines whether data is even available or maintained for analysis. In short, cyber defense is fragmented, creating a disjointed environment in which everyone is fighting alone and losing.

To further clarify why fighting alone causes everyone to lose, a use case compiled from recent attacks is instructive. A private company with a national security portfolio made decisions on its information technology budget, and its acceptance of cyber risk, cost, and its competitiveness. Despite best efforts, due to human error, the company network was compromised. The compromise was only discovered after a third-party cybersecurity company informed the company of the compromise while working with a third company on a similar compromise committed by the same malicious cyber actor.

Given the importance of the company's national security portfolio, the Federal Bureau of Investigation (FBI) was notified and opened an investigation. The Cybersecurity and Infrastructure Security Agency (CISA) was also called because this company supports a portion of the national critical infrastructure, and it too opened a separate investigation. Both agencies'

[2] Most of the details in this section are found in the following reference; other notes come from personal discussions with relevant cyber subject matter experts and the author's own analysis. Joe R Reeder and Tommy Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack," *Cyber Defense Review* (2021), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2723341/cybersecuritys-pearl-harbor-moment-lessons-learned-from-the-colonial-pipeline-r/.

investigations suffered due to a lack of data for analysis. The data was contractually not available, and it was not collected and stored for forensic type analysis by the network owner and network providers. The U.S. Securities and Exchange Commission (SEC) was also notified.

After the victim company eventually received permission to share information from the company's network vendors due to contract clauses, analysts quickly determined that the breach was most likely committed by a foreign cyber actor. In the case of national security systems, there are processes with strict oversight that enable the National Security Agency (NSA) to support the FBI and CISA. However, the foreign cyber actor used a US commercial cloud as part of its infrastructure precisely to obscure its foreign origins, which further complicated the sharing of information between all investigative teams. Days and weeks went by as each entity tried to do their part to navigate legal and procedural restrictions and guidelines to determine attribution, and to remediate the malicious cyber activity on the network. The response was fragmented at best, and reactionary at worst. In the end, each entity involved generated their own understanding of the attack, but the lack of a holistic understanding at speed and scale ultimately meant that everyone had lost. During the same period, the cyber actors moved on to their next victim, also most likely defending alone.

A private company is responsible for the creation, operation and sustainment of its own network using best practices. Going back to the neighborhood analogy, when crime becomes a problem, it is not unusual for a neighborhood watch to be formed as it is one part of a coordinated response that is nested within local, state, and federal legal frameworks. In a related way, a team of teams is required to conduct a holistic cyber defense. So, does it still make sense, from a cyber defense perspective, that private companies are solely responsible for defending their networks?

Returning to General Nakasone's remarks about SolarWinds: no single entity – be it the owner of the network itself and all its suppliers; the government or governments; and the private sector – can see all the dots. Therefore, no single entity can defend itself sufficiently against the threat of cyber-attack The network owners can only see the dots they can see, the private companies that make and operate the networks can only see the dots they can, and the government is likely able to see additional dots that the others cannot (normally in the intelligence and law enforcement fields). Essentially, a fragmented cyber defense prevents any one entity from creating a complete picture of an attack or threat, which leaves everyone exposed and everyone at risk. The lesson we desperately need to learn from recent history is that integrated and coordinated defenses can be effective. Until we coalesce around a common defense framework in cyberspace, we are stuck with a fragmented system. The common rule of thumb should be *when everyone is defending alone, everyone is losing.*

NOTES

Joe R. Reeder and Cadet Tommy Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack." *The Cyber Defense Review* (2021): 15-39, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2723341/cybersecuritys-pearl-harbor-moment-lessons-learned-from-the-colonial-pipeline-r/.

Ally or Die: The Unlearned Joint Organizing Lesson and Key to Survival

Timothy J. White

Joint is better than single service; allied is better than alone; coalition is better than isolation. Neither the United States nor its allies are currently where any would want to be or should be operationally; none are as secure or assured as they should be; and none are performing as efficiently or effectively as required. Given the gravity of national security and the pace of cybersecurity, neither is served by an avoidance of a new call to joining forces in cyberspace. History has repeatedly shown the value of having allies in a tough fight; cyberspace presents that tough fight today.[1]

We can certainly use allies now – across government, private sector, and state partners. The unlearned lesson, however, is that we must organize across common principles and capabilities to create effective alliances for the cyber fight. There is little alternative to going forward: we must learn to ally or we will die. This essay offers learning building blocks, organizing principles, and some concrete future lessons to help cement the effectiveness of cyber allies across the like-minded democracies.

Baseline Building Blocks for Learning Hard Cyber Lessons

The lack of a shared foundation is part of the unlearned lesson. A foundational cyber baseline requires a series of shared and understood building blocks integrated from the beginning in the relationships among allied partners.

Building Block One – Recognize Cyber's 'Overwhelming' Character

Cyber begins at overwhelm. Conventional military kinetic operations are both discrete and linear, and their kinetics are measurable and discernible. While these operations can certainly happen in parallel and together, they generally tend to unfold before they overwhelm. Cyber is experienced more simultaneously as something more ubiquitous and exponential.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Timothy J. White A 30-plus year national security practitioner, strategist, and cyber operations expert leading joint military formations and combined intelligence community organizations. He has commanded at all levels within the Navy and Joint Service, most recently as United States Fleet Cyber Command / TENTH Fleet / Navy Space Command, and previously the Commander, United States Cyber National Mission Force. A former Director of Intelligence for US Indo-Pacific Command, he has served globally in combat zones and conflict areas supporting competition dynamics. He holds diplomas from the U.S. Naval Academy, Naval Postgraduate School, Naval War College, and National Defense University, among others. A former CINCPACFLT Shiphandler-of-the-Year, he misses his days driving a Battleship. He is committed to talent management because up-gunned organizations are made up of up-skilled people. He assesses we are in a race condition, no longer possessing the luxury of time, distance, and accepted international standards as great power competition accelerates.

Building Block Two – Recognize Cyber's Systemic Challenges

Cyber possesses an uncommon degree of persistence, simultaneity, and asymmetry, which is often described with both frustration and good humor. In a graphic novel, a senior military commander or civilian policy maker would say "cyber" followed by a lengthy string of emotive characters – @#$%&!– or grawlix. Six aspects are essential to the shared learning in this building block:

1. **Cyber.** Cyber is analogous to a wild card placed in a search string; anything can be prefixed, appended, or free-associated with cyber and cyberspace. More bluntly, cyber can be distilled down to two data groups that have to be understood. These are the sources and analytics that work with algorithms and aggregators, and the deciders, who are normally human, but increasingly could be artificial intelligence.
2. **Ecosystem and Environment.** Cyber must be considered from at least two basic perspectives: the technology ecosystem and the decision-making environment. The technology ecosystem is the combined hardware infrastructure, firmware, and software that build and connect cyberspace. The decision-making environment is how people, and organizations of people, decide and do – or interact – with and within cyberspace.
3. **Simultaneously Fast and Slow.** Even considering *c* - the speed of light - that governs the top limit of cyberspace campaigns, activity in cyberspace physically can occur impossibly fast. Conversely, given lags in people's responsiveness, it can take a comparatively large amount of time to arrive at a tipping point where action happens. If one has credible and responsible state actors employing a professional target systems approach with a regard for concepts like law of armed conflict and professional trade-

craft, then it still takes many months, perhaps years, of analysis, preparation, movement, and maneuver to execute an exploitation campaign such as the 2020 SolarWinds campaign or the 2021 Colonial Pipeline ransomware campaign.

4. **Attribution and Intent Uncertainty.** Uncertainty over intent or attribution favors the authoritarian or criminal attacker. Bound by a rule of law, democratic defenders will moderate their responses to match the lack of clarity about whether anonymous activity is effective targeted advertising or espionage. Furthermore, both activities could be precursors to a campaign of disruption or destruction.
5. **No cybersecurity but for cryptology.** The national security profession must embrace this mantra as fact. We design, build, and need our national security-related platforms and infrastructure to be secure and available. We are connecting at a distance in order to command/control our military forces in their operations, which requires mission security, assurance, and confidence. These require alignment with, and attachment to, a nation state intelligence community's cryptologic capability; otherwise there is no cybersecurity.
6. **Trust and Identity.** This is about people and their cyberspace interactions with each other, and about the citizens of a country and their agency alongside the sovereignty of a nation and its security. Neither persons nor nations can be taken at face value without confidence in who – and what – is being represented. This is also about trusting our digital identities, which rely on cryptology. Block-chain technology allows for anonymous but highly assured and transparent transactions. Whether that same technology can be leveraged for greater trust in international agreements and alliance remains to be seen.

Building Block Three – Recognize Cyber's Connectivity Pressure

There is only one network, separated in time, which is all connected and inter-connected. Even air-gapped or stand-alone networks will connect to people over time. The tendency to diffuse and connect is the value proposition behind the network effect, which is fundamental to basic information theory. It may take years, but the entropy of the system will drive a logical connection even among those securely separated. This inevitability defines the operating terrain and influences the concept of operations.

Building Block Four – Recognize Cyber's Provenance Dependence

Supply chain and kill chain – don't leave home without 'em. These terms are keyed to a military frame of reference, but you could replace "supply" with "manufacturing" or "research" and "kill" with "market." Whatever your enterprise, it needs to mobilize and aggregate capacity and capability and then deliver to market those goods and services. In a data-driven cybered world, the separation between origin story and end game is governed by the same dependency and vulnerability. If a secure supply chain is lost, then you have handed adversaries advantages throughout their kill chain and crippled your own defense.

In sum, allies need to share similar views of these building blocks to create alliance-friendly organizational designs for national cyber defenses. Intentional organizational definition, structure, and alignment will be our best enablers of success in the unfolding great power competition in cyberspace.

Defending Alone is a Fool's Errand

Joint organizing is key to cyber survival. The term "ally" applies to both inter- and intra-governmental arrangements, which must have sockets for myriad stakeholders to plug into. In this case, the "plug-and-play" aspect of cyber alliances or joint operations becomes an inter-organizational "plug in and help defend" innovation. Like-minded democracies and their constituent organizations must strenuously and jointly learn to design and build their organizations to act on the following tenet: *ally or die.*

Consider the term "ally." It means more than partner or convenience. It means more than integrated operations from planning through execution. It is about establishing common cause with the force of treaty and the consequential power made of binding shared interests and actions. There are plenty of bureaucratic forces and externalities that serve to separate, isolate, and diminish effective security and resiliency; allied causes serve to counter and mitigate these forces. The desired outcomes of coherent strategy, underpinned by allied operations that connect joint forces, public-private partnerships, and the international sphere, are increased capacity and capability; efficiencies in managing escalation and minimizing destabilization; and a dynamic, anticipative posture that capitalizes initiative and sustains momentum. There is agreed consequence and accountability.

To be clear, allied does not mean "the same." Everyone does cyber differently. There is value in this diversity when like-minded partners and stakeholders agree to optimizing principles in pursuit of common cause. One only has to look to the lessons learned from the US approach to joint organization in cyberspace for cyberspace outcomes, which include resilience, security, assured data, and platforms. In this example, military cultures as old as the US Army and Navy - 245 years so far – are now operating alongside the newest Space Force with a displayed unity of action that is both extensible and scalable.

Seven Principles of Organizing with Allies

Mutual cyberspace interests such as national postures oriented on strategy, economic mobilizations, and critical infrastructures coupled with structured, integrated campaigns can be jointly aligned when organizations built on the baseline building blocks continue to observe the following seven cyber and allied organizational principles:

1. **Organize Around Maneuver Principles** – fast and agile. You must think left of reaction and move left of response. In cyberspace, there is no other winning proposition.
2. **Organize for Purpose** – confident, contextual, and frictionless decision making. Cyber moves too quickly for indecision and doubt.

3. **Organize to Generate Outcomes** – enterprise decision making and campaign actions with continuous feedback that sustains dynamic innovation.
4. **Organize to Strengthen Relationships** – culture, behavior, communication, and trust.
5. **Organize to Achieve Common Cause & Shared Goal** – I heard a likely apocryphal story about President John F. Kennedy visiting NASA headquarters for the first time that underscores this principle. During the tour, the president introduced himself to a janitor and asked him what he did at NASA. The answer was simple and clear: "I'm helping put a man on the moon!"
6. **Organize to Generate/Sustain Capacity and Capability** – humanity is living in an increasingly connected, exponentially time-consuming, and attention-deficit disordered world that has nowhere to go but "up" and "more." The world population when the Internet was invented was 3.6 billion, and the number of connected devices was in the single digits. The world population today is more than 7.7 billion, and the number of connected devices today numbers at 13.8 billion, likely approaching 30.9 billion in 2025.
7. **Organize Around a Strategy** – following two decades spent fighting the Global War on Terror and other hot zones, we are now operating under the Great Power Competition strategy of "2+3." Published in 2018, this strategy was of inestimable value. It oriented the executive branch of government, clearly articulated the case for shared interest to allies and partners, underpinned U.S. Cyber Command's (USCYBERCOM) defend-forward and persistent engagement campaign planning; and codified the military services force generation around information warfare. The 2020 Cyber Solarium Commission report, alongside the 2021 establishment and confirmation of the National Cyber Director position, are consistent with recognizing the value of a national strategy. Organizing with allies need just such a clear common strategy as well.

Taken together, these principles enable a unifying multi-stakeholder/organizational/national cyber operational strategy that accounts for respective national interests and goals alongside varied means, and generates an enhanced and collective cybersecurity that ranges from situational awareness to shaping for deterrence.

Five Lessons for Cyber Allies

The better the allies succeed with organizational designs, the closer they will be to having *features over bugs in the national cyberspaces that each will have*. The question will then be how to get closer to optimizing the organizations for defense with respect to boundary conditions of time, terrain, and lethality thresholds, as well as defining conflict categories, adversary numbers and tradecraft, scale imperatives, and the full picture of concrete-to-code-to-context cybered systems.

First, *boundary conditions need to be integrated into allied operations*. Time horizons embedded into allied activities need to be "now through over the horizon," with an understanding of lessons from the past. Terrain lines need to be determined to avoid an incomplete view of compute and cloud. Where does compute happen and where does cloud reside? Or do they reside in the same place? Drawing that line with full allied agreement will allow for more comprehensive strategy development, resource allocation, and decision making. Lethality boundaries need to go beyond the simplistic. For example, drone warfare is not possible without cyberspace and has become a standard tool of modern conflicts. Avoiding complete autonomy is a choice a state makes. However, given the emergence of "full-take" data and "line-speed" decision making, it will be hard not to choose autonomy and automatic if the intent is to achieve maximum effect in cyberspace and kinematic maneuver. Whatever the choice about autonomy, it must be one in which allies commit to operating within the defined boundaries to their fullest extent.

Second, *conflict categories require allied consensus*. Jointly agreeing, deciding, and organizing in advance around conflict in cyberspace will be vital given the simultaneity of time compression and dilation across cyber operations. Consensus will help overcome the difficulty in applying concepts like conventional or strategic deterrence to cyberspace, as well as achieving the systemic benefits in defend-forward persistent engagement. Furthermore, it will enhance an allied nation's ability to manage conflict confusion and escalation by addressing definitional or circumstantial conundrums such as determining what is offense or defense or espionage, if cyber is part of a maneuver warfare campaign, and if there is an existing, recognizable structure. Allied lack of consensus enables the adversary, as a disruptor or spoiler, to diminish or confuse vital interests and reduce allied effectiveness by promoting distorted benefits in sovereign independence and fragmenting allied morale and trust.

Third, *adversary numbers, scale, and tradecraft trajectories* are advancing across the board and require the full spectrum of allied collective attention. Adversaries can be said to be winning the features vs. bugs contest against like-minded democracies whose *bugs (gaps)* are their *features (benefits)* and conversely, their *features (such as strategic coherence)* are the allies' bugs (shortcomings).

Fourth, *organizational alignment and a shared understanding that promotes collective action* is the surest way to address the challenge. A comprehensive target list of adversary campaigns exceeds the scale of any single nation to accommodate even with the best capabilities.

Fifth, *very little across the "Cybered – Cyber" spectrum* spanning the concrete to code to context in the physical, logical, and social world, is truly isolated. The allies must collectively build in security from the beginning and from the ground to top floors of all organizations; ensure integrated visualization and situational awareness; and effectively orchestrate a deliberately structured decision autonomy at machine speed.

The landscape now is more convoluted and distorted than ever. An alliance of problem-solving efforts and decision making within and across governments, alongside our international and private sector partners, is the only way forward.

A Few Final Reflections as Lessons for Like-minded Allies in a Cybered World

The following are two general sets of lessons going forward for cyber allies, drawn from a decade spent embedded in cybered conflict during which my thinking on organizational design and implementation changed as I transitioned from establishing the framework for USCYBERCOM to commanding one joint and one service formation responsible for full-spectrum cyberspace operations. This overview of the lessons is intended to further the thinking for the now and future cyber allies.

Practical Reflections for the Near-Term Future

During my first command of a cyber unit, I had some pre-conceived, and as it turns out, mistaken notions. In my 27 months commanding a Fleet and 21 months commanding our Cyber National Mission Force, I confused mass with capability. This first set of reflections details what I learned from my colleagues' observable mistakes and best practices, that could be coupled with organizational principles to improve our cybersecurity and cyber operations at scale.

- **More than Interactive On-Net Operators.** Operators are necessary, but commanders need as many or more endpoint analysts, developers, all-source analysts, product and infrastructure engineers, and targeteers. We need the enablers that make the hacking possible.
- **More than consuming readiness.** Force generation (up-skill and up-gun, then orient to mission, task, and purpose) of the workforce is critical. Building and sustaining a ready and strategic reserve is vital. This requires training and cycles.
- **Mostly offense is wrong.** The fight is more complex and weighted through Network Operation and defense. It is more about cybersecurity and assured command and control. This is what the adversary thinks they can impact.
- **More than cyber.** The fight is "cybered." That term is really about integrated whole-of-nation-plus information operations and information warfare. These are areas neglected or at least atrophied for some time.
- S**mall, dedicated teams count.** Every member needs to be trained, competent, and qualified. The expectation bar needs to approach exceptional, and it is necessary to start cross-training.
- S**mall, cross-functional teams are the most agile, but you need a lot of them.** Because there is a prioritization and reaction problem, there is always a need for more teams. AI will not solve this challenge (yet). One answer is to build highly trained/qualified active-reserve-civilian small teams, sourced from across the services, formed from aggressive and inquisitive recruiting strategies.

Thinking Forward for the Future

In reflecting on circumstances spanning the summers of 2020-2021 and with an eye to the horizon, we possess several bugs that are currently working to the adversary's advantage. It is wholly within our ability to transform them into features that foreclose adversary advantage.

- Understand the *difference between the skills gap and the discovery gap.* We are fairly good at the former because that looks like training. There is a need to get much better at the latter, which is the product of the curious pursuit of the 'new' that is built on a foundation of critical and creative thinking. Education across allies is key. In the US, the Department of Defense should fully leverage USCC Joint Force Provider and Joint Force Trainer authorities to develop an educational curriculum to supplement the unparalleled training pipeline currently producing our cyber warriors and embrace best practices found within industry, the IC, and allies and partner nations.
- *Acquisition cycles and processes* are abysmal for cyber across allies. Success here looks like sustainable multi-year money and risk tolerance. One method for achieving more transparency and effective oversight would be raising the accountability bar on execution and planning enabled by – at least in the US – fast fail flexibility, among other modernizations. Like-minded democracies are saddled with systems meant for steam-powered equipment and are not currently suited for the speed and scale of change in the digital sector.
- Embrace the reality of a *digital disconnect between open democracies and the ability of adversaries to launch* much of the cyber hacking and associated disruption cost from inside the US. Across the allies, one must somehow reconcile this divide. Are there applicable legal structures from other countries that could be adopted as a pilot? Similarly, allies will need to understand and undertake a large-scale domestic effort to raise awareness about mis- and dis-information.
- Reasonably *solve the information sharing obstacle.* There is lot of classification for national security reasons going on in each nation's cyberspace. We need a hard look that assesses the distinction between what needs to be *classified* versus *protected.* This would both focus on prioritized matters and reveal/unleash a new workforce. Consider how the UK NCSC seems to have successfully integrated common cause and information sharing alongside united government and private sector professionals on a shared national cybersecurity mission.
- The cyber alliance ought to adopt *a professional red-team competitive league* approach. It could be as simple as penetration testing systems (code) and facilities (concrete) or contemplating counter-intuitive or unanticipated alternative scenarios in advance (context). Imagine what a "fantasy cyber red team draft" could look like.

In Closing

All of us have time to confront the threat without kinetically confronting the adversary – for now. If we are to ascribe any value to deterrence, we must agree that deterrence requires readiness, resilience, and organization. Given a commitment to rules-based international order and the opacity that cyberspace brings to sovereignty, identity, and trust, the simple reality is that none of us can do it alone. There is increasing scale, value, and capabilities in allied partnerships and shared perspectives. Organizing teams and commands, bureaus, directorates, and agencies with this in mind will preserve our forward-looking decision space. We must collectively bolster deterrence and move from response to a position of our choosing with an improved readiness posture - together.

Small States Learn Different Survival Lessons

Benjamin Ang

Every state wants to learn lessons from the multitude of cyber incidents that strike it and others, so that it can protect itself in the future. But when international cyber incidents are viewed together with geopolitical contestation, the lessons learned by small states are very different from those recognized by the global superpowers. Large states in NATO or the EU need to understand these other lessons to achieve their initiatives in the UN and elsewhere internationally. This chapter conveys five key lessons from the perspective of one small, highly connected state, and its small state neighbors in Southeast Asia. These lessons need to be recognized by the larger, globally dominant nations which seek the support of, or to support, the smaller nations in global cyber conflicts.

Lesson 1: Small states are often on their own when it comes to cyberattacks.

The 10 member states of ASEAN – the Association of South East Asian Nations – are Brunei, Cambodia, Laos, Myanmar, Vietnam, Philippines, Thailand, Malaysia, Indonesia, and Singapore. The dynamic between states is a major factor in their perception of and response to cyber incidents.

ASEAN has some similarities but is quite different from the European Union (EU) or the North Atlantic Treaty Organization (NATO). Key differences that are relevant here:

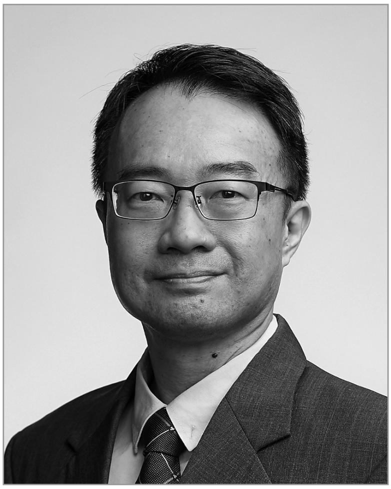
(1) ASEAN is an inter-governmental organization without pooled sovereignty (unlike the EU which is a supranational organization that has pooled sovereignty).

(2) ASEAN has no parliament but has an Inter-Parliamentary Association, and the ASEAN secretariat is not at all as powerful as the EU secretariat.

(3) ASEAN takes all decisions by unanimous consensus instead of votes. (Tommy Koh, 2017)

These differences illustrate that ASEAN member states do not have sufficient common interests, trust, and shared identity to form the collective security framework needed to establish a NATO-type security structure. (Chau Bao Nguyen, 2016) NATO has pronounced

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.



Benjamin Ang is the Senior Fellow leading Cyber and Homeland Defence research at the Center of Excellence for National Security (CENS), a policy research think tank in the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. His team examines how laws and public policy respond to developments in cybersecurity and information and communications technology, international law and norms, technology nationalism, smart cities, artificial intelligence, disinformation and information operations, foreign interference, social media, and emerging technology.

He draws from private sector experience as a former litigation lawyer, CIO, legal counsel, law lecturer, technology consultant, and even Novell Netware Administrator back in the day. He is a trainer for the UN/Singapore Cyber Diplomacy Programme, presented at the United Nations Open-Ended Working Group on Developments in Information and Telecommunications in International Security, and testified before Singapore's Select Committee on Deliberate Online Falsehoods.

that a serious cyberattack on any of its members would trigger collective defense under Article 5. This has been criticized as lacking clarity, but ASEAN states lack even this framework for collective defense. When it comes to cyberattacks, small states are often on their own. This has implications for their response, as we will see below.

Lesson 2: Small states often lack an international response to cyberattacks.

Asia-Pacific states are increasingly vulnerable to cyber threats, with organizations 80 percent more likely than others to be targeted by hackers, but the global median dwell time (time to detection of breach) in Asia is double the global median. (Christy Un, 2020) ASEAN countries have also been used to launch attacks, either because they have unsecured infrastructure which can be exploited or they are well-connected hubs for initiating attacks. (Dobberstein, 2018).

Despite these challenges, only four ASEAN countries have clearly defined agencies responsible for cybersecurity: Singapore (Cyber Security Agency of Singapore), Malaysia (CyberSecurity Malaysia), the Philippines (Department of Information and Communications Technology), and Indonesia (Badan Siber dan Sandi Negara, the Cyber Body and National Encryption Agency). The rest split responsibilities among the ministries of defense, telecommunications, and police. Singapore, Malaysia, Thailand, and Vietnam have national cybersecurity strategies and legislation. Limited progress has been made across the rest of ASEAN. (AT Kearney, 2018 cited in Ang and Raska, 2018) Almost half of the Asia-Pacific states still do not have national cybersecurity strategies in place. (Christy Un, 2020) More details of the state of cyber maturity can be found in reports from the Australian Strategic Policy Institute (ASPI) and EU Cyber Direct.

Cyber resilience of ASEAN states, measured as their ability to deliver the intended outcome continuously despite adverse cyber events, is hindered by lack of policy leadership in some states. Some of the notable cyber incidents in ASEAN states of the past few years have included the following:

1. **Vietnam:** Chinese hacking group "1937CN" took over flight information screens and sound systems in two airports and used them to display propaganda supporting China's rule over the South China Sea.
2. **Philippines:** APT32, also known as OceanLotus, which has been linked to Vietnam, breached ASEAN computers in Manila and compromised government agencies in Philippines, Laos, and Cambodia.
3. **Singapore:** SingHealth, the national health care system, was breached and 1.5 million patients' non-medical personal data were stolen; 160,000 dispensed medicines records were taken, including those of the Prime Minister.
4. **Singapore:** A database of 2,400 Ministry of Defencse/Singapore Armed Forces personnel was breached, by phishing a third party vendor.
5. **Singapore:** A list of 14,200 people diagnosed with HIV was copied by the ex-lover of a doctor who had access to the Ministry of Health database.
6. **Thailand and Vietnam:** Toyota customer data were breached, with no details given.
7. **Philippines:** Personal data of 82,150 customers of Wendy's restaurant were breached.
8. **Philippines:** Personal data of 900,000 customers of pawnshop Cebuana was breached.
9. **Thailand:** Personal data of 45,000 customers of True Corp mobile was breached.
10. **Malaysia:** Personal data of 46 million mobile subscribers were breached.
(Source: CSO Online)

Only the first three cyber incidents have been attributed to nation-states. The rest were classified as cybercrime. Contrast this with Kaspersky's report that at least seven APTs are carrying out cyber incidents for economic and geopolitical intelligence gathering. In none of these cases do we see public diplomacy being used, or indictments being issued, or 'name and shame' exercises being carried out, against the attackers.

Table 1: APTs carrying out cyber incidents for economic and geopolitical intelligence gathering.

APT	Target countries	Target entities
FunnyDream	Malaysia, Philippines, Thailand, Vietnam	High-level government organizations; political parties
Platinum	Indonesia, Malaysia, Vietnam	Diplomatic and government entities
Cycldek	Laos, Philippines, Thailand, Vietnam	Government, defense, and energy sectors
HoneyMyte	Myanmar, Singapore, Vietnam	Government organizations
Finspy	Indonesia, Myanmar, Vietnam	Individuals
PhantomLance	Indonesia, Malaysia, Vietnam	Entities
Zebrocy	Malaysia, Thailand	Entities (source: Kaspersky)

Lesson 3: Small states usually do not attribute cyberattacks.

In the first cyber incident listed, the media attributed the Vietnamese airport attack to 1937CN because its name was displayed prominently on the screens that had been breached, alongside propaganda supporting China's claim to the South China Sea. This was corroborated by reports from FireEye and Fortinet that there was forensic evidence of 1937CN conducting a phishing campaign targeting Vietnam Airlines. Since 1937CN had claimed responsibility for the attack prima facie, there was no need for the Vietnamese government to prove the attribution. Presumably, Vietnam has the forensic or foreign intelligence capabilities to carry out attribution of cyber incidents, but most of the other ASEAN states do not.

In a confusing twist, 1937CN publicly denied involvement in the attack, while reiterating in the same announcement that the South China Sea belongs to China. 1937CN also described itself as a patriotic hacker independent of the Chinese government. The Vietnamese government has neither pressed the issue nor taken any public steps against China.

This does not mean that Vietnam does not conduct acts against China at all. According to cybersecurity firms, the threat group APT32, also known as Ocean Lotus, which cybersecurity firms have linked to Vietnam (some call it "government-backed"), targeted Chinese government officials during the coronavirus outbreak in January 2020 and aimed to compromise the professional and personal email accounts of employees at China's Ministry of Emergency Management and the Government of Wuhan. To be clear, this is far from an official Vietnamese government action.

The second cyber incident listed has been grouped by cybersecurity firms as a campaign by the above-named APT32. All these attributions have been provided by the private sector, not states. According to this attribution, APT32 carried out attacks on three ASEAN websites, websites of dozens of Vietnamese non-government groups, individuals and media, websites of Chinese oil companies, websites of ministries or government agencies in Laos, Cambodia (ministries of foreign affairs, the environment, the civil service and social affairs, and national police) and the Philippines (the armed forces and the office of the president). (Reuters)

Despite the enormous scale of this attack, Cambodia, Thailand, Laos, and the Philippines did not choose to attribute, or in some cases even acknowledge, this cyber incident. The Philippines' foreign ministry said it would look into the report, with the spokesman asserting "Any credible information received will be investigated and addressed as necessary." Cambodian national police said it did not know who was responsible for the hacks. Officials in Thailand said they were not aware of any hacking of government or police websites. (Reuters)

One reason these governments were reluctant to attribute the attacks may be that they lacked the cyber forensic capability to gather enough evidence to substantiate attribution. This is likely to be the case for Thailand, Cambodia, and Laos, although the Philippines is believed to possess such cyber forensic capability. At the same time, FireEye, which very much has the cyber forensic capability to substantiate its claims, very publicly and confidently attributed the attacks to APT32 and linked APT32 to Vietnam. Yet, none of the states adopted this stand.

This brings us to the third case, in which Singapore's national healthcare system SingHealth was breached. The Minister described the leak as the most serious, unprecedented breach of personal data in Singapore. A huge public inquiry was conducted through 22 hearings and resulted in a 454-page report. This has been the most public response to a cyber incident in ASEAN to date.

To understand the context, Singapore is considered a regional thought leader in cybersecurity and was ranked at the top in the International Telecommunication Union's Global Cybersecurity Index (GCI) in 2017. Singapore has published its national Cybersecurity Strategy, which outlines its vision, goals, and priorities, and a four-pillar approach to protect essential services from cyber threats and create a secure cyberspace for businesses and communities. Singapore's Cybersecurity Agency (CSA) is the government agency with a core mission to keep Singapore's cyberspace safe and secure. Singapore has even set up the ASEAN-Singapore Cyber Centre of Excellence with a substantial budget to provide cyber capacity building for its ASEAN neighbors.

Of all ASEAN states, Singapore had the capability of identifying the culprit in this cyber incident. Its response, given by the Chief Executive of the CSA, was instructive: "We have determined that this is a deliberate, targeted and well-planned cyberattack, not the work of casual hackers or criminal gangs... beyond this I apologize we are not able to reveal more because of operational security reasons."

Singapore clearly attributed the attack to a nation-state, but stopped short of identifying the nation-state, much less carrying out any cyber diplomacy response.

To understand this better, the theoretical framework of Baram and Sommers (2019) is helpful. They point out that victims of cyber incidents can either "(1) reveal the attack and attribute it to the alleged attacker, or (2) reveal only the fact that the attack had occurred, without attribution." Some victims may choose to "call out" (publicly identify) the aggressor as flouting international laws and norms, as a "naming and shaming" strategy. They may also do this for deterrence, by demonstrating their technical knowhow in identifying the attack and pointing out the entity behind it, because defensive capability can signal general technological competence and a complementary offensive know-how.

However, Baram and Sommers also acknowledge that some victims choose not to identify their attackers, to protect the safety of their intelligence sources, to prevent escalation because exposure may lead to open confrontation, or for both reasons. Singapore's restricted form of attribution appears to have been for the former reason, and we can speculate that the latter reason is also relevant.

In this respect, Singapore asserted its technical capability in identifying the attacker, which may have some deterrent value. It may also have refrained from publicly "naming and shaming" because of the danger of escalation. Singapore has neither publicly claimed nor denied any cyber offensive capability. For strategic reasons, the risks of cyber conflict to this highly connected nation are arguably too great. There is no known Singapore equivalent of APT32 that would carry out deniable operations.

Even if escalation does not go as far as cyber or armed conflict, it could adversely affect trade relationships. Trade relationships among ASEAN member states, and between ASEAN states and their trade agreement partners, are very important for their economic survival, and are described in further detail below.

Singapore notably did not declare that the incident was in breach of international laws and norms. This is significant because Singapore has been one of the key drivers in ASEAN for adoption of international law and norms for cyber operations, and actively involved in the United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (UN OEWG) and United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE) processes. This may be because Singapore determined that the SingHealth breach was an act of espionage, and there is no general prohibitive rule against espionage under international law.

More recently, in Singapore's public statements about the SolarWinds breach, it also refrained from framing it as a breach of international law and norms. This is possibly for the same reason that it determined the act was espionage. (Eugene Tan, 2021)

Lesson 4: Small states' survival is more dependent on trade than cyber.

ASEAN's growth has come on the back of various free trade agreements (FTAs), some of which are the world largest. The ASEAN-Australia-New Zealand Free Trade Area (AANZFTA) covers 90 percent of goods traded among ASEAN, Australia, and New Zealand, for a population of 653 million and over US$4.3 trillion. Under the ASEAN-China Free Trade Area (ACFTA), China has been consistently ranked as ASEAN's largest investor for a decade, with total trade of over US$731 billion in 2020. The ASEAN-India Free Trade Area (AIFTA) is the world's largest free trade area market, creating opportunities for over 1.9 billion people in ASEAN and India with a combined GDP of US$4.8 trillion, and exports from India to ASEAN were US$31 billion for the 2019-2020 period while Indian imports from ASEAN were US$55 billion. Most recently, ASEAN signed the Regional Comprehensive Economic Partnership (RCEP) agreement on November 15, 2020, with Australia, China, Japan, New Zealand, and South Korea. The RCEP is the largest FTA in history and could add US$186 billion to the global economy as well as 0.2 percent to the combined GDP of its members. (Dezan Shira, 2020)

According to the United Nations COMTRADE database on international trade, Philippines exports to Vietnam were US$1.27 billion in 2019, Vietnam exports to Philippines were US$3.46 billion in 2018, Thailand exports to Vietnam were US$11.61 billion and Thailand imports from Vietnam were US$5.01 billion in 2019. Cambodia-Vietnam trade volume reached US$4.8 billion in 2019, an increase of 14% over the same period last year (https://comtrade.un.org/).

All these statistics point to the importance of trade for the small states in ASEAN. The major cyber incidents have been difficult to attribute definitively and appear to be espionage or propaganda, neither of which is prohibited under international law. Weighed against the risk of damaging trade relations, states may decide that it is better to refrain from escalating matters.

Even if calls are met for an independent, global organization to be set up for investigating and publicly attributing major cyberattacks, it is unlikely that ASEAN states will make use of such attribution in public diplomacy. They could use independent attribution in private back-channel discussions, but we will never know.

Lesson 5: Small states cannot defend forward.

With all the limitations and constraints facing small states in ASEAN, most have their hands full with cyber defense, and the idea of defending forward is beyond them. Unlike the US, most small states have no cyber capacity to seize and maintain the initiative across the competition continuum. The consequences for a small state, if it is discovered inside the network of one of the major cyber powers (US, China, Russia), would be disastrous. The adverse effect on trade if a small state is discovered inside the network of one of its trading partners would also be considerable.

It may also be risky to participate in defend forward or "hunt forward" operations initiated by the US. An ASEAN state (country A) is well within rights if it invites the US (country B) into A's networks to take the initiative against adversaries there. However, if country B uses country A's networks to seize the initiative in the networks of a large adversary (country C), there could be blowback from country C against country A. If country C is a major cyber power and/or a major trading partner of country A, this will not end well for country A.

Unlearned Lessons

The overarching lesson that we can learn is that international cyber incidents, viewed together with geopolitical contestation, have a very different impact on small states as compared to that on the global superpowers, and the calculus for response is very different. This must surely influence the positions of the many small states that populate the United Nations, and their interactions with the UN OEWG and UN GGE processes regarding international law and norms for cyber operations. More research is needed. In the meantime, it would be in the interests of the global superpowers to pay heed to the lessons learned by small states.

Some Things the Giant Could Learn from the Small: Unlearned Cyber Lessons for the US from Israel

Eviatar Matania
Lior Yoffe

INTRODUCTION

Over the last decade, cyber threats have grown in magnitude and diversity, and governments devote massive efforts towards adjusting their cyber stance to the evolving threats of the next decade, developing multiple national cyber strategies and dedicated governmental entities to address cyber threats. The responses build on their own and sometimes other countries' experience. For many small nations, however, modest budgets and resources disadvantage their responses. In contrast, Israel succeeded in becoming a cyber success by deliberately leveraging the advantages of being small – Making quick decisions, having the dexterity to change course rapidly, and centralizing national efforts with relative ease. Israel has focused on organizational processes and thoughtful cyber strategy, offering some lessons that could be useful for other nations that are much larger in scale.

This work focuses on where a small country's approach to national cyber security may be relevant for great powers. We examine this issue through the specific case of Israel's advanced, successful cyber approach, which had been quickly developed and implemented through the last decade, and assess its potential adequacy as lessons specifically for the US. The US is a great power, with an area 500 times that of Israel and a population and economy 50 times that of Israel. Our analysis focuses on which of the major elements that Israel focused on may be independent of scale and could also be adopted by a great power such as the US.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Professor **Eviatar Matania** is a tenured professor at the School of Political Science, Government and International Affairs at Tel-Aviv University, where he heads the MA programs in Security Studies and Cyber Politics and Government, and an Adjunct Professor at Oxford's Blavatnik School of Government, where he convenes the Cyber Module. Professor Matania was the founding head (2012-2017) and former Director General of Israel National Cyber Directorate (INCD) in the Israeli PM office for six years, where he reported directly to the PM and was responsible for Israel's overall cyber policy, capacity building, cyber security strategy, and its implementation to defend the Israeli civilian sector. Professor Matania holds a B.Sc. in Physics and Mathematics (Hebrew University of Jerusalem), an M.Sc. in Mathematics with expertise in Game Theory (Tel Aviv University), and a Ph.D. in Judgment and Decision Making (Hebrew University of Jerusalem).

THE ISRAELI CASE

Over the last decade, Israel has become a cyber-defense power by building its cyber capabilities in all dimensions—a comprehensive cybersecurity strategy, new national and governmental organizations, cyber security operational capabilities, and a cybersecurity leading industry (second only to the US), far beyond its relative global size. In this process, Israel developed a comprehensive approach and implemented it through several governmental resolutions, with a strong correspondence between the vision, the strategy, and the structures.

Aiming for a vibrant and sustainable cyber defense ecosystem, Israel's cyber leaders pursued six objectives:

1) national concept of operations
2) operational national cyber agency
3) cross-sector aid to national cyber robustness
4) collocated and collaborating cyber eco-system across industry, academia, and human capital
5) elite cyber teams for techno-operational problems
6) reorienting on countering attackers, not just attacks

These six aspects effectively combined theoretical and practical approaches to cyber security.

First (Policy): A National Concept of Operation to Deal with Cyber-attacks and Attackers as part of an overall National Cyber Strategy

The basic Concept of Operation (ConOp) was designed to be technology and adversary indifferent (to be sustainable through the years), to be cyber native, and to clearly highlight the government versus the private sector roles. The ConOp is comprised of three layers (Matania et al., 2016; Adamsky, 2017). The first layer deals with fostering Market Robustness against daily threats, reducing the nation's surface attack and overall risks. From a governmental perspective, it is executed

Lior Yoffe is one of the founders of the Israel National Cyber Directorate (INCD), currently serving as its Chief Strategy Officer. Prior to that, Mr. Yoffe held several top executive positions within INCD, including the Executive Director for Threat Intelligence, Head of the Cyber Operations Division, and Head of Defense Planning. Thus, he harnesses his vast experience over the years to tackle national challenges in cyber security: Policy, R&D, and operations. Before joining INCD, Mr. Yoffe held various positions in the cyber community in Israel. He also served as Chief Instructor of Talpiot Program, Israel's elite training program for R&D leadership of the Defense Community. Mr. Yoffe holds a B.Sc. in physics and mathematics from The Hebrew University of Jerusalem and an M.A in Security Studies from Tel Aviv University.

mainly by promoting basic cybersecurity hygiene and guiding efforts taken by the private sector through incentives, regulations, and mandatory standards for critical infrastructure, and engaging in awareness and knowledge raising. The second layer is an event-driven tier that aims to tackle cyber threats as they materialize. It defines the national efforts to achieve Systemic Resilience, which focuses on creating situational awareness, tracking threats, handling and mitigating incidents, and promptly sharing information. This involves directly working hand in hand with the private organizations at risk.

While the first two layers concentrate on mitigating attacks, the third layer focuses on the capacity to disrupt cyber-attacks by focusing on the human factor behind them—the attackers—through national defense capabilities. Namely, this layer involves managing a defensive campaign against state-level adversaries, using all national capabilities, traditional and other, such as intelligence, deterrence efforts, law enforcement, etc.

Second (Policy): An operational Central Cyber Agency for National Cyber Defense

Israel's second step was to create a central cyber agency (now part of Israel National Cyber Directorate or INCD), with concrete operational capabilities and the responsibility to defend the national cyber domain and to lead the national cybersecurity efforts.[1] Its role is to implement the three-tier ConOp in operational activities over all the layers. It starts with the Robustness efforts, directly overseeing Israel's critical infrastructure sector as well as working together with other regulators to systematically raise the cyber hygiene of the whole private sector. It continues with leading the national Resilience efforts, mainly through the national CERT and unique analysis and engagement teams where and when needed to mitigate high-risk threats over the civilian sector.

[1] This need was described thoroughly in the paper "Structuring the national cyber defence: in evolution towards a Central Cyber Authority" (Matania et al., 2017)

Finally, INCD leads the defensive campaign and coordinates combined efforts to tackle adversaries with the police, intelligence community, and other relevant security organizations.

Third (Capacity Building): Enhancing National Robustness

A high level of robustness allows the prevention of potential damage from the most common attacks. It raises the threshold of capabilities, and the effort cyber attackers require to penetrate the nation's cyber domain. As the required investment in each attack step rises for attackers, the number of overall attacks decreases.

The INCD chose to address the issue through several vectors. The most well-known is the Israeli approach towards regulating critical infrastructures (CIs). CIs are directly regulated by INCD in a unique way. Each CI has a certified officer within INCD that is trained and authorized to give professional instructions regarding cyber security. In addition, INCD uses the entire spectrum of the regulatory toolbox when facing the entire private market, such as command and controls, standard setting, the duty of disclosure and disclosure regulation, incentives, nudge solutions, raising awareness in the target audience, and more.[2]

Fourth (Capacity Building): Establishing a Cyber Eco-System of Industry, Academia and Human Capital

The INCD took the lead to build a national cyber ecosystem to strengthen its scientific and technological cyber capabilities and innovation processes in the cyber realm to ensure Israel's long-term cybersecurity capabilities.

For this purpose, the Israeli government, through the leadership of the INCD, supported the establishment of research centers in the universities and their work with leading cyber industries; financed high-risk industrial innovation; invested budgets and efforts in enhancing the nation’s human capital in the cyber field; and fostering an ecosystem for mutual enrichment. The most notable example is the unique CyberSpark project in Be'er Sheva, a concentrated and unique cybersecurity ecosystem consisting of Israeli startups, global companies, academia, and civilian and military cybersecurity centers, all within walking distance of one another.

Fifth (Operational): Cyber Commando: Assembling Small Elite Teams to Tackle Tough Techno-Operational Problems

A working group must be small enough to be efficient. In his remarkable book, Northcote Parkinson defined the "coefficient of inefficiency," implicating the size at which a committee or other decision-making body becomes completely inefficient. While being semi-humorous, Parkinson had a point. This notion is of great importance when a nation-state wishes to address the most challenging problems of cyber defense. The core team must be proficient, small, and agile enough to conduct continuous hunting efforts on an ever-changing adversary and should have top experts on its side. The key point is to have a working task force with top analysts in their respective cyber security field, which tackles tough problem, such as identifying

[2] For additional information on the broad regulatory toolbox see for instance Baldwin et al. (2012).

and tracking Advanced Persistent Threats (APTs) campaigns, in innovating techno-operational ways. Israel, being a small country, is accustomed to the logic of small, highly skilled teams that all fit in a small room together. Naturally, it adopted that kind of thinking also in the field of tough cyber defense challenges.

Sixth (Operational): Dealing with Attackers, not only Attacks.

A key element of cyber threats is the existence of a human perpetrator with malicious intent. Accordingly, the third layer of the Israeli ConOp described above consists of national defense efforts, namely the capacity to disrupt cyber-attacks by focusing on the human factor behind them through national operational defense capabilities. These efforts consist of two main vectors. The first focuses on criminal entities through national and international law enforcement mechanisms, mainly police forces and justice systems, while the second concentrates on state-level adversaries looking to harm national interests, whether terror organizations or other countries.

Israel, as a significant cyber power and a leading nation in this field, also sometimes sets the bar in its approach to dealing with national security issues: In May 2019, during several days of heated fighting with Hamas, the IDF destroyed the building of Hamas cyber unit headquarters using fighter jets (IDF, 2019). This unprecedented kinetic response to a cyber-attack showed a first glimpse of the overall thinking in Israel about the way to deal with cyber attackers. This approach was further demonstrated in the recent Guardian of the Walls operation, where several cyber targets (storage facilities, hideouts, and few cyber terrorists) were attacked by the Israeli Air Force and destroyed (IDF, 2021), thus contributing to the deterrence equation between Hamas and Israel.

WHICH ARE THE POTENTIAL LESSONS FOR LARGER NATIONS?

The six major steps fall into three groups for analysis as potential lessons. These are public policy decisions (the ConOp framework and the centralized agency for national cyber defense), capacity building steps (enhancing national robustness and supporting the cyber ecosystem), and operational related steps (assembling elite teams and dealing with attackers).

The first group, the public policy decisions (ConOp and Operational Cyber Agency), is already in progress in the US. A decade ago, there were only a few national cyber strategies and dedicated governmental cyber departments. However, in the following years, there has been a lot of progress on that front, during which many states published their respective national cyber strategies. The US was one of the first to do so. Nonetheless, when it came to establishing a dedicated nonmilitary and nationally operational cyber agency, the US made a significant step in 2018 when it created the Cybersecurity and Infrastructure Security Agency (CISA), the successor of the previous National Protection and Programs Directorate (NPPD). The mission of NPPD was reorganized and broadened into a new agency and prioritized its mission as the federal leader for cyber and physical infrastructure security (DHS, 2018). By doing so, the US has taken a major step forward in assembling an operational agency dedicated to national cyber defense. Overall, following the 2018 act, we see no crucial and potential lesson that can be adapted from the Israeli case in this group.

The second group, the capacity-building steps (Ecosystem and Market Robustness), responds well to scale if pursued strategically and coherently. In most national challenges, scale naturally benefits the US in these areas where bigger is usually stronger. In principle, the larger scale enables more agencies to work on specialized standards and forces them with their larger budgets and more operational options to go deeper into and across all cyber security research agendas. Where Israel has an advanced and strong regulatory framework, it is due to its security culture where the private sector agrees to specific governmental steps. A good example is the concept of certified officers trained in cyber, assigned to each of the critical infrastructures, and supervised closely by the INCD. However, the lessons are almost impossible to apply to the US, but not for scale reasons. Instead, the relations between the federal administration and the private sector are much different, more antagonistic or disconnected; the ecosystem has to cope with a much different security culture and notions of political interaction.

Finally, the third group, the operational steps (Elite Teams and Attacker-oriented Response), is a much more relevant area to lessons that might be adopted by the US in viewing Israel as a pilot state. This is because operational aspects in cyber usually demand agility, creative thinking, and quick reflexes, therefore, they are easier to achieve in small environments and bodies.

The example of small elite teams created by Israel to tackle national challenges in exceptionally difficult techno-operational questions offers particularly useful lessons for US national cybersecurity success. Israel is not the only example. One can see that creating such elite hunting teams also happens within the global cyber industry. Major cybersecurity firms dealing with threat hunting assembled their respective elite teams—Kaspersky Labs' Global Research & Analysis Team (GReAT), Microsoft Threat Intelligence Center (MSTIC), Google's Threat Analysis Group (TAG), and others. Another example of a task force is Google's Project Zero—the team of top security analysts tasked with finding zero-day vulnerabilities. All these teams had tremendous achievements in their super hard missions despite their relatively small number of analysts, and their continuous publications over the years suggest that it was not a one-time success.

The US should consider creating such elite teams beyond those already in the U.S. Cyber Command (USCYBERCOM) or National Security Agency (NSA) to answer the toughest techno-operational questions found in hunting and tracking APT adversaries. These elite teams should be kept small to maintain their quality and agility. Above all, the lesson from Israel is to provide this commando team with a "shielding bubble" focused on their missions to tackle tough challenges, undisturbed by non-essential organizational politics and managerial interference.

Similarly, there are lessons to be learned from Israel's experience to disrupt and deter cyber attackers. The strikes against Hamas cyber attackers during intense operations provided the first glimpse of a new cyber strategic thinking in dealing with cyber attackers in a unique and unprecedented way in the history of the digital era.

Countering the attackers rather than just the attack is crucial for the overall approach towards cyber threats. Israel has shown a glimpse of its overall efforts and thinking on dealing with attackers through the kinetic response against Hamas in 2019 and 2021, which brought together operational, technological, and legal efforts in a timely manner to tackle attackers and enhance deterrence. This lesson needs to be more explicitly learned by the US. Publicly, the US is currently responding to cyber attackers mainly by using indictments and sanctions. We suggest that, as a world leader, the US should carefully consider a more advanced and comprehensive approach to act against cyber adversaries.

SUMMARY

The following table concludes the major step taken by Israel in its approach to the cyber threat during the last decade and their potential adequacy to the US:

Table 1: Israel approach to the cyber threat during the last decade and their potential adequacy to the US.

#	Category	Step	Is there a lesson to learn?
1	Public Policy	Strategy and ConOp formulation	No. US already has vast strategic thinking
2	Public Policy	Centralized agency for cyber defense	No. Already happening with the establishment of CISA in 2018
3	Capacity Building	Enhance national robustness	No. Scale and security culture differences prevent mutual lessons
4	Capacity Building	Support the cyber eco system	No. Scale and security culture differences prevent mutual lessons
5	Operational	Assembling small elite teams to tackle hard techno-operational issues	Yes.
6	Operational	Dealing with attackers	Yes

Israel owes much of its success in the cyber realm to its ability to flip the disadvantages of having a comparatively small budget and few resources into cyber strategy and process advantages that offer lessons in public policy decisions, capacity building processes, and operational capabilities to other states. As such, combined with its unique geo-strategic position, Israel developed several unique approaches towards cyber security, which offer several lessons for the much larger US.

Much of what Israel has done around cyber strategies and new operational organizations to tackle the cyber threat to the nation, as well as its capacity-building mechanisms are either already handled by the US or require underlying conditions not found in the US, such as universal military conscription. These lessons are either unnecessary or not possible for the US to adopt. However, we find that the US could learn several lessons from the Israeli case by carefully examining its operational decisions and approaches. Those steps are relevant not only for small countries but also for larger, especially for the US. Specifically, the as-yet-unlearned lessons are foster small elite (non-military) groups of national cyber specialists ("cyber commando") to put the US in a leading position to tackle high-end techno-operational cyber-attacks, and publicly embrace a more comprehensive and deterring approach to address cyber attackers.

REFERENCES

Adamsky, D. (2017). The Israeli Odyssey toward Its National Cyber Security Strategy. The Washington Quarterly, 40(2), 113-127.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: theory, strategy, and practice. Oxford University Press on Demand.

DHS, (2018, Nov. 13), "Congress Passes Legislation Standing Up Cybersecurity Agency in DHS". Retrieved from: https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs.

IDF. (2019, May 5). “CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed”. Retrieved from: https://twitter.com/IDF/status/1125066395010699264.

IDF (2021, May 21), "Operation Guardian of the Walls", Retrieved from: https://www.idf.il/en/minisites/operation-guardian-of-the-walls/second-week-summary/.

Matania E., Yoffe L., Goldstein T. (2017), “Structuring the National Cyber Defense: In evolution towards a Central Cyber Authority”, Journal of Cyber Policy, Volume II, Issue 1, Chatham House.

Matania, E., Yoffe, L., & Mashkautsan, M. (2016). A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy. Georgetown Journal of International Affairs, 17(3), 77-84.

Policy and Organization Unlearned Lessons

Paradigm Change Requires Persistence - A Difficult Lesson to Learn

Dr. Emily O. Goldman

Persistent engagement and defend forward are new cyberspace concepts and approaches that are gaining traction across the cyber enterprise. They challenge the assumptions and prescriptions of deterrence theory and thus require perseverance in ensuring the right lessons are learned. Claims by some that SolarWinds represents a failure of these approaches misses the mark in many respects, most of all by applying deterrence metrics inappropriately. Rather, recent experience has demonstrated that competition in cyberspace is going to be continuous. Competing requires persistence rather than episodic responses, and anticipation rather than reaction.

2018 Shift

When future historians look back at 2018, they will see it as a pivotal year in the evolution of the United States' (US) cyberspace strategy. The unlearned cyber lessons from previous years took form in strategy and policy in 2018. US political leaders, operational commanders, military strategists, and scholars worked out a theory about the nature of cyberspace conflict and competition, how to confront national-security threats emanating from cyberspace, and ways to employ cyberspace capabilities as a tool of national power. Persistent engagement and defend forward are new cyberspace concepts and approaches that challenge the previously dominant assumptions and prescriptions of deterrence theory and thus require perseverance in ensuring the right lessons are learned and applied. Experience has demonstrated that competition in cyberspace will be continuous. The lesson is that it requires persistence rather than episodic responses, and anticipation rather than reaction.

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018–19. From 2014 to 2018 she directed the U.S. Cyber Command / National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command vision, *Achieve and Maintain Cyberspace Superiority.* She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University and was a professor of Political Science at the University of California, Davis, for two decades. Dr. Goldman has published and lectured widely on strategy, cybersecurity, arms control, military history and innovation, and organizational change.

In March 2018, U.S. Cyber Command (USCYBERCOM) released its *Command Vision* introducing the concepts of defend forward and persistent engagement. In September 2018, the U.S. Department of Defense (DoD) declared in its new cyber strategy, “We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict,” and “[p]ersistently contest malicious cyber activity in day-to-day competition.” Defend forward and persistent engagement pivoted US cyber teams from a “response force” to a “persistence force” and represented the shift from a coercive strategy aimed at preventing cyberspace attacks by threatening to impose costs on bad actors to an initiative-persistent strategy aimed at thwarting and frustrating adversaries before they lock in gains.

This new conception of operations in cyberspace supplemented the longstanding coercion paradigm that still holds sway in policy deliberations among strategic theorists and practitioners alike. The legacy coercion framework views strategy in terms of deterrence and compellence, even though deterrence was advanced during the Cold War to address a novel and acute problem: how to secure with nuclear weapons when you cannot defend against them. Deterrence thus rests on credible threats to impose costs to influence the adversary’s cost-benefit calculus to deter or compel their behavior. In cyberspace, however, the opponent’s calculus is a given: they are expected to persist because entry costs are low, attribution is not timely, redlines are ambiguous, and pervasive system vulnerabilities invite exploitation for strategic gain.

Insights Gained and Accumulated into Broader Lessons

We are beginning to grasp early lessons from this shift in strategic thinking for cyberspace. The operational approach of persistent engagement emerged from Operation Glowing Symphony (OGS), USCYBERCOM’s first global-scale operation to persistently disrupt and degrade ISIS media infrastructure. General Paul Nakasone (then Commander of Joint Task Force-Ares) observed that one of the first things learned during OGS was that threats are not going to stop after one engagement. Rather, they will be continuous and require persistence. The operation lasted seven months and dramatically reduced the scale and speed of the virtual caliphate's media voice. Operational learning has thus informed learning at the policy and strategy levels. Consider this a primer on insights gained over the past five years. What have we learned?

1. Cyberspace is strategically consequential and US adversaries seeking strategic effects from cyberspace operations do so to defend themselves against perceived "Western" ideological (i.e., liberal democratic) subversion of their regimes, to resist sanctions, and to advance their interests at US expense. Operations and activities in and through cyberspace enable dictators and other bad actors to affect sources of national power (thus having strategic impact). They seek to protect their regimes through continuous campaigns of cyber operations, including the theft of intellectual property at-scale to reduce the economic advantages of the US and its allies, supply chain disruption and manipulation, and theft of Western military R&D to erode military superiority in key technologies. Disinformation and information manipulation undermine political cohesion in the West, delegitimizing democratic institutions and processes, and harming alliances. Since strategic effects can be achieved through actions short of war, authoritarian states and non-state actors will continue to experiment in this cyber competitive space, whether we respond or not. The bottom line is that cyberspace competition is strategically consequential, not because it could be a step toward escalation to armed conflict. Thinking about competition principally as a step toward war misses how actions in competition can secure strategic victory before ever approaching the war-fight.
2. In cyberspace, gains are cumulative. Any single action, hack, or incident alone might not be strategically consequential, but cumulatively the results can be of great strategic impact. It is insufficient to concentrate on preventing significant incidents or catastrophic attacks during ongoing campaigns comprised of activities whose individual effects never rise to the level of a significant incident, and therefore rarely elicit a timely response, yet which cumulatively produce strategic gains.
3. Cyberspace campaigns against US and allied interests are continuous and ongoing across space and time, so too must our approach be to thwarting them. There is no operational pause. This does not mean being everywhere all the time; it does mean that the struggle to retain the initiative in cyberspace is enduring. As General Nakasone explained, "Superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral. That's why we must operate continuously to seize and maintain the initiative in the face of persistent threats." This requires a campaigning mindset that recognizes security and stability in cyberspace flow from deliberate, cumulative action, not the threat of prospective action.

4. Being assertive and active does not mean being aggressive or offensive. Much of the activity associated with defend forward allows the US to be anticipatory about resilience, in other words defending forward in time. It often employs defensive measures undertaken with consent of the system or device owner and/or the state in whose territory cyber infrastructure resides. Yet enhancing resilience—as necessary as it is—is insufficient by itself. Action does not undermine stability; rather, restraint in the face of continuous aggression is destabilizing because it incentivizes aggressors to continue to operate with impunity and leads to de facto norms antithetical to our interests and values. Unlike nuclear weapons, the strategic effect of cyber capabilities comes from their use, not their mere possession.

5. Fears about escalation have not materialized. We have yet to see escalation out of the cyber competition space into armed conflict. Adversaries have been emboldened—arguably, by our restraint—but emboldened behavior within the cyber competition space is not the same as escalation out of competition and into armed conflict. We have demonstrated that we can preclude and disrupt cyber aggression without escalating to armed conflict.

6. Cyberspace operations have become a standard tool in diplomacy and competition between states. Restraint above the armed attack threshold occurs alongside routinization below that threshold in continuous campaigns of non-violent operations. And what works to deter catastrophic or armed-attack equivalent cyber-attacks has not dissuaded adversaries from routinely operating in and through cyberspace for strategic influence. Cyber aggression below armed conflict is not an anomaly but rather signals the emergence of a new competitive space where agreement over the substantive character of acceptable and unacceptable behaviors is immature. The lens of persistent engagement views as normal occurrences what many policymakers describe as deterrence strategy failures.

7. What matters most in cyber strategic competition short of armed conflict is not that capabilities are forward, but that cyber forces are engaging and seizing initiative. Defend forward is not synonymous with "forward defense" or "forward positioning" as practiced by the US and NATO during the Cold War, when troop presence near international borders signaled readiness and enhanced deterrence. Defend forward is not about messaging through force posture and disposition. It is about actively operating and engaging to shift the balance of initiative in one's favor, and upon gaining initiative (i.e., defending forward in time), to structure the playing field and force the opponent to play on a field that better suits your strengths.

8. The reflexive use of impose cost in cyberspace strategy and policy is misplaced. Because of the strategic imperative to be active in cyberspace, our energy and resources would be better spent precluding adversary options for exploitation rather than trying to alter

their cost-benefit calculus to act. The objective should be to shift the composition of the adversary's portfolio of cyber activities in a manner that benefits us.

9. Redlines are notoriously difficult to define in cyberspace. Adversaries have been adept at designing their intrusions and disruptions around the redlines we defined only after we endured earlier intrusions and compromises. Calls for setting redlines leaves us one step behind and always reacting while opponents set the timing, tempo, and terms of competition.

10. Metrics designed for the coercion/conflict space do not fully apply in competition. The metric of success for defend forward and persistent engagement is not the absence of action, but rather sustained initiative that constrains the adversary's freedom of maneuver and renders their actions strategically inconsequential. We should be anticipating how we will be exploited, taking away exploitation opportunities from the adversary that are likely to result in strategically consequential effects, and setting the conditions of security in cyberspace to support our interests and values.

Principles of Cyberspace

Paradigms reflect deeply held, taken-for-granted assumptions about how the world works, which can cause lessons to remain unlearned for some time. Outdated paradigms are difficult to change—despite mounting evidence that their utility has declined. Sanctions, indictments, expulsions, designations, and naming and shaming can all in principle constrain an adversary's freedom of maneuver by exposing bad behavior, but they are not likely to impose sufficient costs to deter (prevent from acting) or compel (stop acting). Response *per se* does not deter; only responses that outweigh benefits can change the perceptions and behavior of an ideologically motivated actor. Labeling every response as "cost imposition" does not make it so. Relying on redlines and responding to incidents after-the-fact have not stemmed malicious cyberspace activity, and there is no reason to believe such measures will suddenly dissuade authoritarian sponsors of cyber misbehavior. More of the same will not produce different results—no matter how often senior leaders call for a coherent deterrence strategy for cyberspace.

The cyber strategic environment with its dynamic terrain, regenerating capabilities, low entry costs, anonymity, pervasive vulnerabilities, and prospect of cumulative gains rewards continuous action, initiative-seeking, and sustained exploitation. From this list, we can derive key principles to guide cyberspace policy, strategy, and operations, thus implementing the key lessons-to-be-learned. In this case, seven principles borne of experiences are now readily available.

- Superiority in cyberspace is temporary and advantage favors those with initiative; thus, we must operate to seize and maintain initiative.
- One-off cyber operations are unlikely to defeat adversaries; thus, we must compete continuously.

- Continuous campaigns of non-violent operations in and through cyberspace can have strategic effects; thus, we must compete now as well as prepare for future crisis and armed conflict.
- If we are defending inside our networks, we have lost initiative; thus, we must defend forward, outside our system boundaries, as close as practicable to the source of malicious activity.
- Toeholds must not become beachheads; thus, we must hunt on our networks rather than wait for intrusions to become compromises.
- Gains in cyberspace are cumulative; thus, we must employ a campaigning mindset rather than treat incidents and intrusions as discrete events.
- The strategic value of cyber capabilities lies in their use, not their possession; thus, we must act with precision and be risk informed, not risk averse.

In sum, the overarching lesson to be learned is to persevere with persistence across all seven principles.

The views expressed in this article are those of the author and do not reflect official positions of the Department of Defense or any U.S. government entity. More extensive development of the core arguments and lessons appears in Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence: Redefining National Security in Cyberspace, (forthcoming, Oxford University Press, 2022).

All That Which Is Old, Is New Again – Unlearned Lessons about Metrics of Success in Cyber

Harvey Rishikof

In September 2009, the ABA Standing Committee on Law and National Security, the National Strategy Forum, and the McCormick Foundation held a workshop assembling approximately 35 experts on national security threats in cyberspace. The 46-page report, *National Security Threats in Cyberspace*, explored the then cyber threat vectors, legal frameworks, organizational questions and what the future would bring, among other topics. Our reporter was Paul Rosenzweig; as always, he captured the essence of the discussion – and we ended the report with a chapter on the "Metrics for Success." In short, all that was old is new again – this report is almost 13 years old, but all the metrics remain relevant and the same, and sadly, to a great extent, the metrics reflect policies not met.

For the purposes of this discussion, I have reproduced Chapter 6 of the report in italics and made comments and responses in normal text.

> ***Metrics for Success***
>
> *The system today is in a crisis. That crisis is one that is only slowly becoming clear and achieving public awareness – but we stand at a crossroads.*
>
> *Today, determined adversaries can enter some classified systems undetected, encrypt data while in the systems, extract it, and leave behind autonomic tools that will dial back to the installer, over time, at a time of his or her programmatic choosing. That is an immensely serious concern. And if that can occur on classified systems, imagine what is happening in the unclassified domain.*

These are solely the opinions of the author and do not reflect the views, policies or thoughts of any private or government agency.

Harvey Rishikof is the Chair of the American Bar Association Standing Committee on Law and National Security Advisory Committee Chair. He is the former dean of the National War College in Washington, D.C., where he also chaired the department of national security strategy. Mr. Rishikof was a senior policy advisor to the Director of National Counterintelligence, ODNI, legal counsel for the deputy director of the Federal Bureau of Investigation, and dean of Roger Williams School of Law. Currently, he is also an advisor to the Harvard Law Journal on National Security and serves on the Board of Visitors at the National Intelligence University. He is also a Member of the National Academy of Sciences Commission on Law Enforcement and Intelligence Access to Plain Text Information in an Era of Widespread Strong Encryption: Options and Tradeoff. He recently co-authored The National Security Enterprise: Navigating the Labyrinth.

This statement remains true; we still are in crisis – see OPM hack, Microsoft Exchange, Solar Winds, Colonial Pipeline, Ransomware, etc. Nonetheless, this "crisis status" has continued since the last report. We have had some responses, like the public Stuxnet attack, for which no country takes credit, but by and large there have been few public responses to attacks in general and few consequences for our adversaries. The Biden Administration has made cyber a priority with the appointment of an excellent team, but the jury is still out on how effective they can be.

Most kinetic threats we will face can be thought about well in advance and can be prepared for. The cyberthreat will be executed in millisecond time with enduring consequences. If the Chinese military were at our borders ready to attack, we would deem that a crisis. Today, in the cyber domain, we are effectively at the same place. Questions remain:

- *How will we know when the crisis is over?*
- *How will we know if what we are doing is effective?*
- *How do we know if we've won?*
- *Or, put another way, given President Obama's commitment to the creation of a new "Cyber Czar" position within the White House, how will we know if the czar has succeeded?*

These are the fundamental structural questions for our system. One "czar" has come and gone, and yet based on the key fundamental questions we remain adrift. A new "czar" has been proposed by the latest NDAA of 2021 and has been appointed. Although an excellent choice, it remains unclear how effective the new Czar will be.

In asking these questions, we want to move away from traditional Washington metrics of success. By these standards, the czar will succeed if the staff and budget increase exponentially. The czar will be a real bureaucratic success if a fight with some in-house adversary is won.

And the czar will be a failure if some cyber-Pearl Harbor occurs on his watch and the czar is forced to resign.

Consequesntly, we have witnessed the OPM breach, Election hack of 2016, Solar Winds, No-Petya. Should I go on? Who has been held responsible, accountable, or fired?

None of these , of course, is a real measure of success. They assume a myopic "inside the Beltway" vision of reality in which only press releases count. Real success will be difficult to measure. We cannot, for example, say whether a reduction in the number of intrusions detected reflects our success in preventing them or a growing capacity on the part of the intruders to evade detection. Indeed, our only true measures of success are likely to be indirect ones that serve as proxies for our ultimate goal. Nevertheless, if we were to suggest some realistic measures by which our success over the next 4-8 years could be measured, the following would be a non-comprehensive list of metrics that ought to be considered:

Have we reduced the number of intrusions into American governmental systems?

- ❖ *What degree of success do NSA red teams have in penetrating our networks?*
- ❖ *Are we more effective at the attribution of malicious actors?*
- ❖ *Have we improved encryption standards?*
- ❖ *Does intrusion detection lead seamlessly to immunization and prevention, such that intrusions by a particular method are a one-time-only occurrence?*
- ❖ *Have we adopted an effective identity management system (more or less premised on the one outlined in Homeland Security Presidential Directive-12)?*
- ❖ *Is America more successful in offensive cyber intrusions than its opponents are (i.e., are America's offense and defense better than that of our opponents)?*
- ❖ *Have we enhanced coordination and agility in responding to events in a way that makes a Cyber Czar no longer necessary?*

This set of questions has answers that remain opaque and somewhat underwhelming– we are good at penetration but so are our adversaries; we are concerned that quantum physics will undermine encryption; attribution as the holy grail has improved but remains elusive; detections have not led to "seamless immunization and prevention"; we do not have an "effective identity management system"; the general consensus remains that offense beats defense; not only have we not solved the coordination problem but yet again in legislation we have called for a new "czar."

Has the private sector adopted appropriate security measures?

- ❖ *Have we increased the application of patches for vulnerabilities that are known to exist, where lethargy has delayed or prevented application?*

- *Are auditing schemes generally in place?*
- *Have they resulted in the adoption of generally accepted best practices that embody standards of care that the courts deem significant?*
- *Is private sector R&D increasing?*
- *Is there an appropriate liability regime in place that allows injured parties to seek compensation for consequential damage?*
- *Have we found ways to incentivize resiliency?*
- *Are we devising a more secure system architecture for the cyber domain? What are the prospects for its adoption and implementation?*

Again we have a disappointing set of responses to these questions; patches are faster as we move to the Cloud, but due to our movement to the widely adopted systems or clouds the ability to compromise trust has let to systemic attacks; the auditing schemes are not robust; the courts have not ventured into the space with much enthusiasm; R&D is increasing but the breadth of the attack surfaces have made the increase not meet the threat; again no, there has not been established a liability regime; again no, more calls for resiliency have been made but we have not used – tax codes, insurance premiums regulation, litigation or international treaties to reinforce a policy of resilience; we have launched for DIB companies a Cybersecurity Maturity Model Certification process but the role has been deeply problematic and the NIST/ISO framework has only gone so far.

Have we developed a doctrine of cyber warfare and response?

- *Do we know how we will respond to an overt cyber-attack that causes physical damage?*
- *Do we know what our response will be to a covert intrusion?*
- *Have we defined what constitutes an armed attack and when we will attribute that attack to a state actor?*
- *Has the law of armed conflict reached consensus on the definitions of lawful and unlawful use?*

Recently, U.S. Cyber Command (USCYBERCOM) announced its new doctrine of “Defend Forward” to generate effects in cyber against adversaries below the level of armed conflict, but it still is unclear what ultimate effect this new policy will have; the “grey space” or actions below the threshold of an armed conflict has become a cottage industry for the legal community of scholars but still remains open to debate; in short we have no shared consensus on “lawful and unlawful” use of cyber tools. There needs to be a proper forum to construct such a consensus; moreover, the tension between espionage and traditional military affairs or Title 10 v. Title 50 remains a continuing issue.

Have we improved international cooperation against cybercrime?

- *Are international requests for assistance routine and effective?*
- *Is information shared internationally quickly enough to have effect?*
- *Are the numbers of safe havens for cybercriminals being reduced?*
- *Is there international agreement on norms of behavior that have the effect of modifying the behavior of state actors?*

Although we have had some movement on international agreement regarding cybercrime, we still use as our domestic statue the Computer Fraud and Abuse Act of 2005 (18 USC 1030), since revised most recently in 2014; the process under the Mutual Legal Assistance Treaty (MLAT) remains notoriously slow and safe havens for cyber criminals remain; moreover, the UN Group of Governmental Experts process has grinded to a halt since major players such as China and Russia remain recalcitrant about the appropriate roles of international norms.

Have we internalized within the US government conceptions of cybersecurity that are currently lacking?

- *Does procurement policy take account of cyber vulnerabilities?*
- *Are there new federal acquisition rules that incorporate cybersecurity standards for all hardware?*
- *Does OMB fund cybersecurity projects adequately?*

As mentioned, we have launched for DIB companies a Cybersecurity Maturity Model Certification process, but the rollout has been deeply problematic and the NIST/ISO framework has gone only so far; the government's Einstein 1, 2. 3 cyber defense frameworks have not proven to be an effective defense; OMB neither has adequately funded nor overseen a regulated an effective defense for USG.

Have we taken leadership of the cyber issue?

- *Is there a national strategy in place that identifies roles and responsibilities throughout government and in the private sector? Is it a paper strategy or is it actually being implemented?*
- *Does the American public understand the scope and nature of the cyber problem?*
- *Do they care about it, and have they considered how cyber issues impact privacy and civil liberties?*
- *Have we changed the public's mindset on cybersecurity so that good practices are well accepted (much like wearing a seatbelt is now considered the norm)?*
- *Is more attention being paid to cyber conflict in the service academies?*
- *Has transparency increased, thereby enhancing public debate on the appropriate solution set?*

Although we have had the excellent Cyberspace Solarium Commission report (2021), and the commissioners have been effective in having several recommendations become part of the 2021 NDAA, it is unclear how the public views cyber security. There has not been an effective national strategy. Since 1997, we have had 13 cyber-related national strategies issued almost every two years, with three in 2018 alone. Most reports recommend the following reforms: better policies; better public-private practices; improved information-sharing; more centralized coordination and control; better practices for threat sharing of vulnerabilities; more agile and adaptable policies; legal reforms; improved training and education; more R&D; capacity building; and, the establishment and promotion of norms. In short, we have been saying and recommending the same solutions for last the 23 years. (see "From Solar Sunrise to Solar Winds: Two Decades of Cybersecurity Advice," by Michael Tanji). As an aside, during this period of time social media companies have revolutionized the information space and built a multi-billion-dollar market for personal digital data.

- *And the single key metric, which is almost immeasurable:*

HAVE WE EXERCISED VISIONARY AND COURAGEOUS POLITICAL LEADERSHIP TO FORMULATE A COHERENT POLICY?

No, though we have been admiring and writing about the problem for decades. The lessons about metrics remain unlearned. In short, we have yet to establish an effective policy and doctrine of deterrence for cyber. Hope springs eternal and all hope the Biden Administration will be successful where those before have failed.

Powering the DIME: Unlearned Lessons of Asymmetric National Power in Cyberspace

Dr. Michael Klipstein
Dr. Pablo Breuer

The United States (US) has a long history of proportional and in-kind response to adversary aggressions. If a US aircraft is shot down, the US will bomb anti-aircraft emplacements and runways or attain air superiority by clearing the skies of other fighter aircraft. If hostile actions are committed in cyberspace, the US will respond with limited cyberspace actions in an attempt to restrain escalation to a kinetic conflict. The US has failed to learn the lesson that conflict in the cyber age is inherently asymmetric and that cyber attack responses need not be quid-pro-quo. There is a range of diplomatic, economic, and information options for effective responses that follows the international legal principle of proportionality and do not necessarily result in escalation to the kinetic actions of warfare. The US should use, and be willing to target in others, all the DIME instruments of national power – i.e., diplomacy, information, military, and economic[1] - to respond to and prevent future aggressions in cyberspace.

Information Flows and Defense of Democracy

There is a vital relationship between information and democracy. In order for a democracy to survive, citizens need valid information to make informed judgments. As Hamilton noted over 200 years ago in the Federalist papers, citizens of a democracy must be educated.[2] They need to have a substantiated and shared understanding supporting the legitimacy of their elections and their government, in addition to a reasonable expectation of economic security.[3] With these foundations in place, a democracy can use contested political knowledge to identify, understand, debate, and solve problems. Conversely, autocratic governments require a monopoly on common political information to keep the system opaque and their citizens under control.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Dr. Michael Klipstein has worked on national cyber topics for over a decade, ranging from USCYBERCOM continuity of government networks, the National Security Agency hard targets, leading a Cyber National Mission Team, and building two Nation Cyber Protection Teams. Later, he created curricula for the Joint Staff for international partner nations in cyberspace, and was a Director of International Cybersecurity Policy for the National Security Council.

Information flow and mass communications remain fundamental to a healthy modern and internetted democracy. If the majority—or even a significant minority—of citizens do not share a common acceptance of elections, legitimacy, economic fairness, and government, democracy is threatened. Likewise, if there are not enough common objectives and some sense of cohesion, the citizens cannot achieve effective pluralities or majorities that underpin policy, and chaos will follow. Conversely, if there is not enough contested information because, for example, government officials allow access only to their interpretation of facts, then citizens do not have access to the marketplace of ideas, debate, and economic innovation. This can lead to tyranny. Examples include government control of information in numerous regimes, and the Kim Family Regime in North Korea isolating the population from outside ideas to forestall rebellion. Democracy depends on the unhindered flow of information balanced between commonly accepted and contested interpretations.

Among the world's consolidated democracies, the US is particularly vulnerable to attacks that affect the free flow and accuracy of electronically exchanged information. First and foremost, very few countries rely on cyberspace as much as the US. Vast portions of national critical infrastructure in the US are connected to the open Internet. Attacks in and through cyberspace are inherently asymmetric in nature. There are simply more critical cyberspace capabilities that the US must defend than there are for adversaries. Further, the capabilities the US must defend are generally more critical to national security than those its adversaries must defend. Finally, unlike many adversaries, much of the US critical infrastructure is commercial; adversaries typically nationalize critical infrastructure and therefore, can more easily enforce both cooperation and compliance.

In today's world, new forms of disinformation present an urgent national threat to the health of our

Dr. Pablo Breuer is a non-resident senior fellow of the Atlantic Council's GeoTech Center and twenty-two-year veteran of the U.S. Navy with tours including military director of U.S. Special Operations Command Donovan Group and senior military advisor and innovation officer to SOFWERX, the National Security Agency, and U.S. Cyber Command as well as being the Director of C4 at U.S. Naval Forces Central Command. He is a DoD Cyber Cup and Defcon Black Badge winner and has been on the faculty at the Naval Postgraduate School, National University, California State University Monterey Bay, as well as a Visiting Scientist at Carnegie Mellon CERT/SEI. Pablo is also a co-founder of the Cognitive Security Collaborative and coauthor of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

democracy-sustaining information environment. The US is at a distinct disadvantage if it limits responses largely to military-borne cyber operations and excludes the other DIME tools – i.e., information, economics, and diplomacy. For example, in a competition limited only to the cyberspace domain, it is likely that the US has more critical capabilities to lose than its adversaries. These capabilities are not limited to just physical critical infrastructure, but include the fundamental underpinnings of our democratic way of life. Conversely, authoritarian adversaries already controlling their internal communications structures can more readily tolerate major losses of access to the free and open internet to protect their critical infrastructure, as well as preventing the significant loss of connected infrastructure.

Only by fully employing its DIME capabilities can the US learn how to bolster its international support and deter adversary nations from conducting offensive cyberspace actions.

DIME Tools of National Power - D

Diplomacy is the domain of the Department of State. Through discussions and agreement of international norms of accepted behavior in cyberspace, the US can lead the world diplomatically. When the US announces a meeting, other states want a seat at the table. This latent power was most recently needed when the 2017 United Nations Group of Governmental Experts on cyberspace failed to reach a consensus on international norms.[4] Increased adoption of norms of acceptable behavior would enable more clearly defined activities. With such norms established—including a consensus on prohibited targets and activities such as masquerading as other nations or launching critical infrastructure attacks leading to civilian deaths—states could better act without ambiguity or fear of argument over whether their actions are a transgression. Similarly, they will benefit from a common understanding of which activities—like espionage—are allowable.

If better equipped, staffed, and authorized to do so, the Department of State then could more effectively, frequently, and likely more persuasively use existing interagency coordination mechanisms to 'demarche' (protest) the attack and the attacker. A good example is the demarche associated with the 2019 Russian attack on Georgian television networks.[5] This "naming and shaming" via demarche in a public forum notifies the global community of the actions and the potential remediation, and it shapes the information environment. Importantly, it also allows the US to build international leverage by partnering with the affected nation for remediation, training, or multilateral response. More is needed to capitalize on the potential of cyber diplomacy: "*The United States should regain the initiative in strategic cyber competition. The Department of Defense has pivoted to a more assertive posture, but the State Department's pivot has just begun.*"[6]

DIME Tools of National Power - I

Adroitly orchestrating the Information tool of the DIME is crucial to effective governmental responses to adversary cyber campaigns. Evidence collected and shared to support the claim that an attack occurred and attribute the attack or campaign to an attacker helps undermine the inevitable denials or counterclaims and misrepresentation of facts by the attacker or its proxies. As the world's nations increasingly rely on a smoothly functioning global internet for commerce, communications, and critical resource supplies, the public revelations of these attacks and their sources has slowly begun to shape the perspectives of states previously resisting attribution to any state, let alone China or Russia. Identifying states clearly shown to threaten the functions of these global information flows can, depending on the circumstances, coalesce sentiment against those states. For example, the 2013 release of the unclassified APT-1 report by the commercial cyber firm Mandiant provided public and substantial evidence of Chinese cyber operations against the US that enabled its leaders to counter PRC denials of having conducted such offensive military action.[7]

In cyberspace, attacks are increasingly less likely to be isolated events, and more likely to be parts of wide-ranging campaigns with larger economic or national security implications. The 2020 Russian SolarWinds attack exemplifies what Russian General of the Army Valery Gerasimov identified in 2013 as the principles operationalizing for the information age the 1990s anti-US Primakov doctrine. Now clearly stated, the Russian state intends to achieve its national objectives through cyberspace and information operations, intertwining conventional and asymmetric means in a whole-of-government, all domains, and permanent conflict between peace and war.[8] As the authoritarian adversaries to democracy have grown into their many and far-reaching cyber campaigns over the past decade, calls among the targeted democracies have led to cooperative cyber defense agreements and training with the US. In providing persuasive information to reveal the adversaries' campaigns and to encourage cooperative support, the US can measurably enhance the effectiveness of its own cyber defense.

DIME Tools of National Power - M

Global militaries now recognize cyberspace as an operational domain with the ability to hold adversaries at risk without firing shots, deploying forces, or launching hostile kinetic actions. Military actions here may include taking control of hard and soft information resources within the adversary's territory, interfering with understanding or effective execution of military or other sectoral movements, or even manipulating the sentiment of population segments to turn against the ruling regime. "*The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. ... All this is supplemented by military means of a concealed character.*"[9] Early to engage across domains, the military of Russia, led by its intelligence unit – the GRU,[10] has been deeply involved in cyber-attacks on the US and Europe, as has the Chinese People's Liberation Army – the PLA, most recently through its Strategic Support Forces.[11]

Conversely, in the not-distant past, the Department of Defense would conduct cyber training and online operations with only a select few nations. This was due primarily to a lack of statutory authority to train partner nations in cyberspace activities. Since 2018, the Department of Defense now has had greater autonomy to operate in response to threats and, now with the passage of the 2021 National Defense Authorization Act, and through modification of Section 333 of Title 10,[12] it has the authority to train foreign nations in both defensive and offensive cyberspace operations. This expansion of mil-to-mil cyber coalitions similarly expands the options for national cyber defenses beyond more traditional military operations and the narrower scope of the early cyber era in the 2010s. This now-allowed activity sets conditions to partner with and train less capable nations and build partnerships and alliances, furthering US influence globally.

DIME Tools of National Power - E

Economically, nations are reliant upon the internet for commerce. In 2018, the Council of Economic Advisors conservatively estimated in a 2018 report that malicious cyber activity cost the US economy between $57 billion and $109 billion.[13] This number greatly expands when considering the economic impacts from malicious cyber activity online. Over the course of 2020, cybercrime globally increased to levels never seen before. The average loss from a data breach in the US reached $9 million dollars. Losses from IP theft and ransomware attacks included lost market value, downtime, and reduced productivity.[14]

The economic value and vulnerabilities of the global transport sector are a particular case of lessons yet to be learned and national power yet to be appropriately employed. The 2020 National Maritime Cybersecurity Plan cites numerous examples of the reliance and interconnectedness of nations in cyberspace that extends to their economic dependence on shipping. Non-cyberspace disruptions, such as the recent blockage of the Suez Canal, stopped as much as 30% of the world's container shipping daily resulting in an estimated $400 million each hour of blockage, along with disruption of supply chains. To illuminate the scale of the backlog, 421 cargo ships had to wait to transit the canal; the largest of these has the capacity to carry 24,000 20-foot containers.[15] If a cyber-attack could precipitate a blockage of the canal, significant damage to global commerce would occur. Similarly, a cyber-attack on the Panama Canal could significantly delay the US from shifting military power, as well as commerce, between oceans. The loss of the Panama Canal would result in increasing the voyage between New York and Los Angeles by over 7,000 miles. Critical maritime supply chains are equally vulnerable to cyber losses and disruptions, as are land systems.[16]

One would expect this economic reality both to alert national domestic action and to elevate attention to the economic tools of national power. Nations cooperatively seeking to improve cybersecurity of often overlooked systems, such as critical infrastructure, would in principle greatly improve economic resilience in cyberspace and reduce the potential monetary cost of malicious cyber activity. However, the lessons of national power and cyber defense in economic terms are at best variably understood. China has demonstrated repeatedly its grasp of the national value of economic warcraft such as its IP theft policy of "rob, replicate, and replace,"[17] pushing victimized firms out of their own markets, and its oft-used economic bribery or blackmail policies against other nations whose citizens displease Chinese leaders.[18]

The US still lacks a comprehensive plan to secure its critical infrastructure with an anchor organization able to implement a cybersecurity strategy nationally, and has yet to create a coordinated and effective use of its economic power for overall cyber defense. The last tool in DIME is, for the cyber era, one of the least well developed.

Putting the Whole DIME Back in the Game

Continued symmetric actions in an asymmetric space leaves the US at a distinct disadvantage. Adversaries seek advantages through manipulation of the internet and its connected activities and potentially strike at the soft underbelly of open societies in an ever-connected world. Unable to reconstruct the internet for security, the US must use all resources and instruments of power to deter adversaries from meddling in information systems in the private and public sectors. By combining Diplomacy, Information, Military, and Economic actions in response to or in advance of attacks, and while the US is still the leading power in the world in all four elements, the US is well-placed to be more effective, efficient, and resilient in deterring adversaries while also strengthening partnerships and alliances among like-minded nations. But the lessons have to be learned, the tools employed, and the policies needed to act recognized clearly and refined smartly. There is not much time left.

NOTES

1. T. Kodalle et al., "A General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model," *Journal of Information Warfare* 19, no. 2 (2020).
2. Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers* (Yale University Press, 2009).
3. Henry Farrell and Bruce Schneier, Common-Knowledge Attacks on Democracy (October 2018), Berkman Klein Center Research Publication No. 2018-7, available at SSRN: https://ssrn.com/abstract=3273111 or http://dx.doi.org/10.2139/ssrn.3273111.
4. Arun Sukunmar (July 4, 2017),T*he UN GGE Failed. Is International Law in Cyberspace Doomed as Well?* Retrieved April 2, 2021 from https://www.lawfareblog.com/un-gge-failed-international-law0cyberspace-doomed-well.
5. J. Rudnitsky, N. Chrysoloras, and H. Bedwell, February 20, 2020, Russia Blamed for *'Paralyzing'* Georgia Cyber Attack in 2019, retrieved April 2, 2021 from https://www.bloomberg.com/news/articles/2020-02-20/russia-blamed-for-georgia-cyber-attack-that-raises-sanction-risk.
6. Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy (Fall 2020)," *Texas National Security Review* (2020), https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/.
7. APT Mandiant, *APT1 Report: Exposing One of China's Cyber Espionage Units* (February 2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf: Mandiant Ltd, February 13 2013.

8 Eugene Rumer, T*he Primakov (Not Gerasimov) Doctrine in Action - the Return of Global Russia,* Carnegie Endowment for International Peace (June 5, 2019), https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

9. Molly McKew, September/ October 2017, *The Gerasimov Doctrine*, retrieved April 2, 2021, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.
10. Lilly Bilyana and Joe Cheravitch, "The past, present, and future of Russia's Cyber strategy and forces," paper presented at the 2020 12th International Conference on Cyber Conflict (CyCon, Talinn, Estonia, https://ieeexplore.ieee.org/abstract/document/9131723).
11. Elsa B. Kania and John K. Costello, "The strategic support force and the future of chinese information operations," The *Cyber Defense Review* 3, no. 1 (Spring 2018), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR_V3N1_SPRG2018_Complete.pdf?ver=2018-05-02-141744-830.
12. 2021 National Defense Authorization Act, Section 1201, retrieved April 2, 2021, https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf.
13. Executive Office of the President, "Council of Economic Advisers Report: The Cost of Malicious Cyber Activity to the U.S. Economy," *https://publicintelligence.net/us-malicious-cyber-activity-cost/,* February 2018, https://publicintelligence.net/us-malicious-cyber-activity-cost/, accessed August 2020.
14. Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of CyberCrime,* CSIS and McAfee (2020), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
15. Aaron Clark, Cindy Wang, Ann Koh, and Verity Ratcliffe, 2021, "The Suez Canal Blockage Is Over. Time to Add Up the Damages." https://gcaptain.com/blocked-suez-canal-cost-economy/.
16. Eric de Bodt, Jean-Gabriel Cousin, and Marion Dupire-Declerck, "The CSR Supply Chain Risk Management Hypothesis Evidence from the Suez Canal Ever Given Obstruction," available at SSRN 3867169 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3867169.
17. Smith and Lostri, *The Hidden Costs of CyberCrime.*
18. Simon Sharwood, "Chinese database detailing 2.4 million influential people, their kids, their addresses, and how to press their buttons revealed - Compiling using open source intel [and 10-20 percent not open source] hailed as showing extent of China's surveillance activities [Shenzhen Zhenhua company, China]," *The Register online*, September 15 2020, https://www.theregister.com/2020/09/15/china_shenzhen_zhenhua_database/.

Writing the Private Sector Back into the Defense Equation – Unlearned Lessons

Dr. Andrea Little Limbago

Global supply chains received a one-two punch in 2020. The ongoing US-China trade war and COVID-19 made it clear that the increasingly complex, fragile, and opaque global supply chains were no longer sustainable. These significant shocks, coupled with the SolarWinds supply chain compromise and growing concerns over data security and digital supply chain risk, have caused many in the private sector to rethink their global footprint. These global transformations also create a rare opportunity to rethink the role of the private sector in national security.

For the most part, the private sector has been omitted from the defense equation despite being on the frontline of adversarial behavior and geopolitical conflict. In a recent testimony, Senator Angus King explained, "many smaller companies, particularly in Silicon Valley and in the technology field generally, have given up on the Pentagon."[1] When US tech giants withdraw from participation in Pentagon programs,[2] while others aid in the massive surveillance and human rights violations in China,[3] the divide between technologists and policymakers may seem too vast to mend. Nevertheless, closing this gap is a national security imperative. Just as the global order is undergoing transformations, so too must the role of the private sector in national defense.

The window of opportunity for bridging this gap is now. However, as Amy Zegart and Kevin Childs explain, fixing this divide requires thinking differently.[4] To be sure, for the last decade, the private sector largely dismissed any role in national security – and vice versa. Even following Russian interference in the 2016 US Presidential election, many tech leaders were slow to comprehend how their technology could be abused by adversaries.[5]

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Andrea Little Limbago is a computational social scientist specializing in the intersection of technology, national security, and information security.

As the Vice President of Research and Analysis at Interos, Andrea leads the company's research and methodology regarding global supply chain risk, with a focus on globalization, cybersecurity, and geopolitics. Andrea is a Co-Program Director for the Emerging Tech and Cybersecurity Program at the National Security Institute at George Mason, an industry advisory board member for the data science program at George Washington University, a non-resident fellow at the Atlantic Council's GeoTech Center, and a board member for the Washington, DC chapter of Women in Security and Privacy (WISP). Andrea previously taught in academia, was a technical lead at the Department of Defense, and Chief Social Scientist at Endgame and Virtru.

Andrea earned a Ph.D. in Political Science from the University of Colorado at Boulder and a BA from Bowdoin College.

Fortunately, times are changing and private sector leaders from across industries are reassessing their global footprint and how geopolitics impacts their bottom line. This article considers the forces driving the private sector's nascent transformation toward resilience in a post-pandemic global order and how the defense community must seize the moment to redefine public-private sector relations and optimize US national security.

Lessons Unlearned: Thinking Differently about the role of the Private Sector in National Security

These high-profile divides have dominated headlines for the last decade and obscured underlying shifts across the private sector when it comes to national security. The notion of private-public partnerships generally receives strong support, but the frameworks for these partnerships have barely evolved since the Cold War. Even when discussing the Silicon Valley/DC divide, it is largely framed with a focus on bridging a gap between technologists and policymakers through joint research and development, misaligned acquisition processes, and workforce solutions.

While addressing the divide between technologists and policymakers is essential, it is a well-known problem with emerging or nascent solutions. Governmental programs such as the Defense Innovation Unit and DefenseWerx were created to facilitate these partnerships and expedite innovation and technological transitions. Conversely, there are a growing number of programs to recruit more technologists into policy, such as the Aspen Tech Policy Hub,[6] TechCongress,[7] and the National Security Institute Technologist Fellowship.[8] Additional bug bounty programs such as Hack the Pentagon and Hack the Capitol further seek to bring these groups together to address an array of national security and technology challenges, while the Biden administration is experimenting with new approaches to hiring tech talent.[9] The emergence of these programs over the last decade is a welcome change and highlights some lessons learned. Although there is still plenty more work to do, there are a growing number of programs working on it.

In contrast, there has been much less attention devoted to the broader private sector and its role in national security. The private sector is increasingly described as the frontline in cybersecurity, but little has changed in policy or in partnerships despite their growing role as defenders. Of course, there are examples of the government and corporations working together – for example to bring down bot networks – but these are few and far between when looking at the scale and scope of the threat.[10]

For instance, the financial sector is a well-known target of state and non-state adversaries and is among the sixteen critical infrastructure sectors designated by the U.S. Department of Homeland Security.[11] A BBC report highlights a financial 'fraud epidemic' as a national security problem due to both its destabilizing impact on society as well as being a source of funds for terrorist and criminal networks, not to mention the growing number of state and non-state actors that target the financial industry.[12] The fifteen other critical infrastructure sectors similarly are on the front lines of cyber warfare, but rarely get the attention or the resources needed to defend against nation-state attacks.

In fact, given such policy stagnation in addressing the technological realities of the threat landscape, many US and European corporations are now trying to shape global cyber norms. Microsoft's call for a "Digital Geneva Convention" and the Tech Accord, Siemen's Charter of Trust,[13] and Intel's draft US privacy law[14] illustrate this growing movement by corporations to shape the digital rules of the road. Importantly, the growing number of companies signing these accords or seeking similar initiatives demonstrates the growing overlap between national security initiatives and corporate bottom lines.

Of course, the private sector is extremely heterogenous, with great diversity among those corporations that internalize how national security may impact them and those who prefer to maintain a blind eye to it. While there has been policy inertia on the government's side, there has equally been those in the private sector who continue to discount the impact of national security threats on their bottom line. In discussing China's long-time campaign to tamper with technology products, a former FBI official recommends, "Silicon Valley in particular needs to quit pretending that this isn't happening."[15]

To be sure, many on both sides remain wedded to Cold War analogies and private/public sector models from anachronistic eras. Nevertheless, there is also growing acknowledgement of the ongoing inflection point and transformation in the global order which is prompting many in the private sector to rethink their relationship with national security. The next section explores the driving forces behind these shifting attitudes in the private sector regarding geopolitics and national security. This growing momentum introduces an opportune moment to rethink the role of the private sector in national security.

Global Shocks to the Bottom Line

For the private sector, the bottom line will generally trump national security considerations. This will not change. What has changed is the growing convergence of the bottom line and national security, a convergence that introduces great opportunities for reinventing private sector contributions to the defense equation. This section details those core factors behind these shifting attitudes in the private sector.

COVID-19 and Global Supply Chains (globalization reformed)

Beyond the public health and economic devastation, Covid-19 has exposed significant vulnerabilities in a hyper-globalized system, largely the complexity, opacity, and insecurity of global supply chains. From the well-documented food and vaccine distribution and personal protective equipment disruptions to manufacturing and defense supply chains, modern supply chain fragility has now become a top C-suite and consumer concern alike.

Last year, the Bank of England predicted the pandemic would cause the worst economic contraction since 1706.[16] Global economic activity ground to a halt in March 2020, dropping 30-35% in a few weeks. Global GDP forecasts dropped from 2.4% in February to −4% in March, UNCTAD predicted a 30-40% contraction in foreign direct investment flows,[17] while unemployment numbers quickly surpassed the Great Recession and approached Great Depression levels. The April 2020 jobs report detailed a massive jump in US unemployment to 14.7%,[18] as over 20 million people suddenly lost their jobs. This one-month shift was double that during the entire 2007-2009 Great Recession.

While the economy currently is making greater progress than the dire predictions of Spring 2020, the shock will forever transform the global economy. Those who anticipated a return to 'normal' in the post-pandemic global order will be in for a rude awakening. H.T. Goranson and Beth Cardier best detail this risk, noting, "The fact that our smartest scientists and political leaders are envisioning a return to 'normal' reflects a collective failure of imagination."[19]

For the private sector, the global supply chain disruptions linked to geographic dependencies – mainly geographic concentration in China – was a wake-up call. Many companies did not realize the extent to which their extended supply chain was so fragile, with 98% of executives noting some level of supply chain disruption due to COVID-19.[20] In preparation for the future shocks, 24% of companies plan to relocate supply chains, only 10% said China was stable for long-term sourcing, and 50% plan to identify alternative or backups.[21]

In short, while past private sector priorities focused on market access to the world's largest consumer base, the pandemic exposed the underlying fragility of this approach and prompted many in the private sector to begin transforming their global supply chains toward greater resilience.

Industrial Policy is Back

As the Internet exploded, the notion that borders do not exist in cyberspace became a common refrain. The same was often said of globalization, as goods flowed across borders at unprecedented levels. In both cases, national borders were always there, but were either discounted or completely ignored in favor of the potential promise of new market share and growth. This risk calculus is changing, as ongoing trade policies and data sovereignty laws have brought borders front and center to the business world.

While COVID-19 accelerated the push toward greater geographic diversification of global supply chains, the US-China trade war had already prompted a nascent focus on reshoring and onshoring. The 2019 Kearney U.S. Reshoring Index recorded a record high, indicating a growing number of companies shifting their dependencies away from a few core Asian countries toward other regions.[22]

The notion of trade wars is actually too restrictive, as both China and the US are deploying a range of tools in their economic statecraft toolbelt. Industrial policy is back with the business community caught in the crossfire yet again. For instance, the U.S. Department of Commerce has added over 350 Chinese companies to their entity list, which prohibits the export, re-export, or in-country transfer of their products.[23] The Cybersecurity Maturity Model Certification (CMMC) is one of many U.S. Defense Department efforts to secure its supply chain and incorporates security standards into its acquisition process.[24] Through Section 889 of the National Defense Authorization Act (NDAA) of 2019, the Federal Acquisition Council (which includes the Department of Defense, NASA, and the GSA) has restricted federal contractors from using the products from five Chinese companies, and their affiliates and subsidiaries. Separately, from June 2020 to January 2021, the Pentagon issued four different lists – and a total of 43 Chinese companies – with links to the Chinese military pursuant to Section 1237 of the 1999 NDAA.[25] This statutory requirement specifies that the Pentagon must release the names of "Communist Chinese military companies" but there is no compliance requirement. However, a November 2020 Executive Order[26] restricted investments in 31 of the 43 companies listed, and the 2021 NDAA introduced Section 1260H, which supersedes section 1237.[27]

In response, China has sanctioned[28] three US defense companies to signal opposition to US arms sales to Taiwan and the growing trade partnerships between the US and Taiwan – a partnership focused on ties among like-minded democracies with "shared values that will inform how we reinvent the supply chains of the future."[29] China also has announced new details regarding their 'unreliable entity list' — companies deemed to be a danger to China's national sovereignty, security, or development.[30]

While the US and China continue the tit-for-tat retaliatory economic policies, democracies across the globe are starting to leverage industrial policy to secure their own supply chains. Australia,[31] Italy,[32] Sweden,[33] UK,[34] Germany,[35] and India[36] are among the growing list of countries restricting Huawei from their 5G cellular infrastructure. India has taken additional steps, banning over 100 Chinese apps following military conflict along the Chinese/Indian border.[39] The EU recently introduced[40] details for a U.S.-EU tech alliance, while the UK has proposed[41] a 10-country 5G pact of democracies (D-10). Members of the UK parliament also introduced the creation of a trusted suppliers list that would ban China and Russia from the defense supply chains.[42] In fact, many former members of the Soviet bloc are especially wary of Chinese influence and are blocking Chinese projects from the Baltic to the Adriatic. A Lithuanian member of Parliament summarized these decisions succinctly in noting, “We are choosing the Western technosphere. We are not choosing the Chinese technosphere.”[43] These regulatory dynamics introduce yet another supply chain risk for global corporations that increasingly shapes their calculus when restructuring their global footprint.

Data at Risk

At the end of 2020, the SolarWinds supply chain attack revealed just how vulnerable the digital software supply chain is across Fortune 500 companies and the public sector alike.[44] Far from being unique, the SolarWinds attack is part of a broader trend where legitimate software and third-party suppliers provide the attack vector for compromise. These kinds of ‘next-gen’ attacks jumped by 430% year over year.[45] A recent survey found that 60% of data breaches were the result of supply chain or third-party exposure, while most do not monitor all their suppliers for cyber risk.[46]

The physical supply chain also introduces cyber risks that have largely been ignored for the last decade but are beginning to enter the risk calculus. The diffusion of digital authoritarianism – the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations – introduces new data risks for global supply chains.

Whether through data sovereignty laws, Internet blackouts, or ‘cybersecurity’ laws that mandate government access to data within their borders, any private sector footprint within these countries faces much greater risk of data exfiltration and service disruption. For instance, Cambodia is moving toward an autarkic Internet inspired by China’s Great Firewall,[47] while Vietnam[48] and Thailand[49] both passed cybersecurity laws that give the government greater control of data within their borders. Ecuador’s all-seeing eye surveillance system[50] is already powered by Chinese technologies, while Kazakhstan’s required digital certification[51] has proven to enable man-in-the-middle attacks numerous times.

At the same time, government-induced Internet shutdowns are similarly on the rise. Uganda, Belarus, Russia, and Myanmar are among the growing list of governments deploying this technique for information control within their borders. India has also adopted this technique and holds the record for a democracy with the longest Internet shutdown at over 100 days. There were 213 documented incidents of shutdowns across at least 33 countries in 2019 alone.[52] In 2020, governments cut off the Internet to 268 million people – 93 shutdowns across 21 countries – a 49% increase in total hours from 2019.[53] According to the Business Continuity

Institute's Supply Chain Resilience Report,[54] these kinds of Internet disruptions are the most top-of-mind disruption concern for almost two-thirds of organizations surveyed. Government-led Internet blackouts increased 6000% between 2011-2018,[55] and cost the global economy $8 billion in 2019 alone,[56] and likely increased in 2020.[57]

Taken together, national borders dramatically impact data risk. Increasingly for the private sector, where you stand depends on where your data resides. With the average global brand having tens – if not hundreds –of suppliers across the globe, and a large portion of their data distributed across the supply chain, data abroad is increasingly data at risk. But those risks are not uniform and have instigated a growing emphasis on building trusted networks within the public and private sectors.

New Priorities and Solutions for Post-Pandemic World Order

This confluence of shocks has forced a reckoning with geopolitics and the private sector. To be clear, this is not a uniform reprioritization, but those who restructure their operational resilience around these risks will gain the competitive advantage in the post-pandemic world order.

For instance, Intel's new CEO describes the company as "..., a national asset. This company needs to be healthy for the technology industry, for technology in America."[58] With chip manufacturing front and center in the technology supply chain disputes between the US and China, this framing may become more commonplace for other businesses in the tech and critical industries.

This renewed national corporate pride is not limited to the US. Porsche recently announced[59] it would not expand production with a Chinese factory, opting for a Made in Germany approach despite higher labor costs. This came at the expense of lower growth in China in 2020 compared to competitors, and it is still too early to tell whether market pressures or geopolitics will dominate decisions across the auto industry.

At the same time, there are growing shifts toward crafting trusted supply chain networks – both digital and physical – and especially for a democratic 'tech alliance.'[60] The US is weighing a democratic economic alliance[61] that would retaliate in response to Chinese coercive trading policies, such as those used recently against Australia.[62] In addition, trustworthy networks are foundational to these tech alliances and are a growing priority among democracies.[63] The 'quad allies' – Australia, India, Japan, and the US – are stepping up tech ties to strengthen their security and coordination in critical supply chain and technology areas.[64] Creating these alliances will take time and are in a very nascent, exploratory phase but are essential to supply chain diversification, agility, and security.

The movement toward trusted supply chains also has introduced the potential creation of "trust zones"[65] that would share research and technology, while excluding those entities deemed security risks. There also is growing emphasis on industrial policy to formalize these trusted networks, whether through new prohibitions and restrictions to address the semiconductor chip dependencies,[66] national strategies to identify choke points in emerging technology supply chains, as well as through trusted alliances.[67]

Coordinating these restrictions and prohibitions across countries would have several advantages, including a unified front against adversaries, incentivized and increased information sharing, as well as the consistency necessary for private sector compliance. Governments should also consider financial incentives to facilitate compliance given the enormous difficulty and costs of replacing many of the prohibited technologies or reshoring to trusted locations. According to one assessment, it will cost US small carriers $1.8 billion to 'rip and replace'[68] existing Huawei and ZTE equipment from their networks. A German estimate predicts an even larger cost, closer to $3.5 billion for their largest telecom provider.[69] Non-compliance fines also can be extremely costly. OFAC issued over a billion dollars in violation fines in 2019.[70] In July 2021, the FCC approved a $1.9 billion program to expand its reimbursement plan[71] to assist in the compliance costs of removing prohibited technologies from US telecommunications networks. Japan has designated over $2 billion to their domestic champions to facilitate decoupling from the Chinese market.

Additional incentives and protections for information sharing will be essential across these trusted networks. While the SolarWinds attack has expedited[72] information sharing, it was in fact reactionary. A recent report from BSA, The Software Alliance, to the Biden Administration highlights the essential role of information sharing both domestically and with foreign partners, but laments that the government still lacks an effective means for two-way information sharing six years after the Cybersecurity Information Sharing Act was passed.[73] A core component of information is ensuring the data is protected, and given the growth in supply chain attacks, there is reason for concern. Therefore, data protection and more coherent data protection strategies across the democracies must similarly be foundational in securing the 'trust' in information networks.

Finally, the government should craft assurance policies to incentivize companies that pursue best practices for protecting their intellectual property and technology across their supply chains, including qualified bidders and qualified manufacturers lists. This, in turn, should spark a reckoning within US companies as well, especially among tech giants who currently power[74] many of the surveillance capabilities[75] on the US restricted lists, including those with military end-users. To be clear, this does not require a complete decoupling – that is neither practical nor advantageous – but rather incentivizing specific behavior for improved security across supply chains. When that does involve decoupling, government assistance could go a long way. A U.S. Chamber of Commerce report[76] estimates full decoupling would cost hundreds of billions of dollars, lost jobs, lost economies of scale, lost innovation, in addition to completely crippling certain industries. Finding this delicate balance between national security and economic security and welfare requires assurance-based support informed by both the private and public sectors, with each internalizing the practicalities and realities of a post-pandemic world order.

CONCLUSION

When the pandemic hit, numerous private sector companies shifted or expanded production capabilities, for example from athletic gear to masks and gowns,[77] 3-D greeting cards to face shields,[78] and pickup trucks to ventilators.[79] This begs the question: what role would the private sector play during other shocks, such as a large-scale military conflict?

There are many areas of disagreement between Silicon Valley and policymakers, but there is also growing alignment between the private sector writ large and national security concerns. The private sector continues to bear the brunt and costs of global supply chain disruption. From cyber-attacks to shifting data surveillance laws to geo-economics to geographic concentration risks, the private sector is caught in the crosshairs of these global shifts and is reassessing its global footprint for greater operational resiliency.

Geopolitics increasingly play a role regarding where and with whom the private sector purchases technology and which companies are integrated into their supply chain. The push-pull factors of geopolitical and industrial policy shifts are directly impacting their risk calculus and bottom line. The ongoing supply chains disruptions introduced by the COVID-19 pandemic have further prompted renewed thinking within the private sector about geographic and product concentration risks.

The confluence of these revelations provides an opening for democracies to reinvent the role of the private sector in the defense equation. As many global brands are reassessing their global footprint and the range of risks involved, many of these shifts increasingly align with national security objectives. From seeking locations with greater data protection to building operational resilience with trusted partners, there is increased opportunity for collaboration across the private and public sectors. However, this will only be possible by pushing aside the lessons unlearned of the last decade. National security and the corporate bottom line can go hand-in-hand, but it will require renewed focus and forward leaning solutions on par with the geopolitical, geoeconomic, and technological challenges of the post-pandemic world order.

NOTES

1. "Department of Defense Nominee Touts Senator King's Leadership on Cyberspace Solarium Commission." February 2, 2021, https://www.king.senate.gov/newsroom/press-releases/defense-department-nominee-touts-senator-kings-leadership-on-cyberspace-solarium-commission.
2. Billy Mitchell, "Google's Departure from Project Maven was a 'little bit of a canary in a coal mine'," FEDSCOOP, November 5, 2019, https://www.fedscoop.com/google-project-maven-canary-coal-mine/.
3. Liza Lin and Josh Chin, "U.S. Tech Companies Prop Up China's Vast Surveillance Network," *The Wall Street Journal,* November 26, 2019, https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846.
4. Amy Zegart and Kevin Childs, "The Divide Between Silicon Valley and Washington is a National Security Threat," *The Atlantic*. December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.
5. Casey Newton, Zuckerberg: the idea that fake news on Facebook influenced the election is 'crazy,' *The Verge*, November 10, 2016, https://www.theverge.com/2016/11/10/13594558/mark-zuckerberg-election-fake-news-trump.
6. Aspen Tech Policy Hub, https://www.aspentechpolicyhub.org/.
7. TechCongress, https://www.techcongress.io/.
8. George Mason University National Security Institute, https://nationalsecurity.gmu.edu/technologist-fellowship/.
9. Katie Malone, Hide and Seek: Biden administration gets creative recruiting tech talent. *CIODive*, January 20, 2021, https://www.ciodive.com/news/biden-source-code-usds-white-house/593686/.
10. Microsoft Defender Security Research Team, "Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andormeda), Microsoft Blog, December 4, 2017, https://www.microsoft.com/security/blog/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/.
11. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors.
12. https://www.bbc.com/news/business-55769991.
13. Charter of Trust, https://www.charteroftrust.com/.
14. "Intel publishes third draft of federal US privacy law recommendations," *IAPP Daily Dashboard*, May 29, 2019, https://iapp.org/news/a/intel-publishes-third-draft-of-federal-u-s-privacy-law-recommendations/.
15. Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," *Bloomberg*, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/.
16. D'Souza, Deborah. "Bank of England Predicts Worst Contraction since 1706." *Investopedia*. https://www.investopedia.com/bank-of-england-predicts-worst-contraction-since-1706-4844284
17. "Coronavirus could cut global investment by 40%, new estimates show," *UNCTAD,* March 26, 2020, https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2313.
18. Heather Long and Andrew Van Dam, "U.S. unemployment rate soars to 14.7%, the worst since the Depression era," *The Washington Post,* May 8, 2020, https://www.washingtonpost.com/business/2020/05/08/april-2020-jobs-report/.
19. H.T. Goranson and Beth Cardier, "Recovery is Not Enough," *Project Syndicate,* December 11, 2020, https://www.project-syndicate.org/commentary/building-intrinsic-reslience-against-future-shocks-by-h--t--goranson-and-beth-cardier-2020-12.
20. "COVID Resilience Report: The Impact of COVID-19 on Supply Chains and How Businesses are Preparing for the Next Shock," *Interos,* October 1, 2020, https://www.interos.ai/project/interos-2020-survey/.
21. A.B. Brown, "BDO: 24% of companies plan to relocate supply chains" *CFODive*, https://www.cfodive.com/news/cfo-outlook-survey-reshore-supplier-technology/593438/.
22. "Global Pandemic roils 2020 Reshoring Index, shifting focus from reshoring to right-shoring" *Kearney*, https://www.kearney.com/operations-performance-transformation/us-reshoring-index.
23. Bureau of Industry and Security, U.S. Department of Commerce, Entity List, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.
24. Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/.
25. "DOD Releases List of Additional Companies, In Accordance with Section 1237 of FY99 NDAA," https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

NOTES

26. “Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People’s Republic of China,” June 3, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.
27. “DOD Releases List of Chinese Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021,” June 3, 2021, https://www.defense.gov/News/Releases/Release/Article/2645126/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260/.
28. Joe McDonald, “China to Sanction Boeing, Lockheed and Raytheon over Taiwan Arms Sales,” *DefenseNews,* October 26, 2020, https://www.defensenews.com/global/asia-pacific/2020/10/26/china-to-sanction-boeing-lockheed-and-raytheon-over-taiwan-arms-sales/.
29. Reuters Staff, “US, Taiwan seek ‘like-minded’ democracies in supply chain shift from China,” *Reuters,* September 4, 2020, https://www.reuters.com/article/us-taiwan-usa-trade-idUSKBN25V1DC.
30. Evelyn Cheng, “China releases details on its own blacklist, raising uncertainty for foreign businesses, *CNBC,* September 21, 2020, https://www.cnbc.com/2020/09/21/china-releases-details-on-unreliable-entity-list-raising-uncertainty-for-foreign-businesses.html.
31. “Huawei and ZTE handed 5G network ban in Australia” *BBC,* August 23, 2018, https://www.bbc.com/news/technology-45281495.
32. Giuseppe Fonte and Elvira Pollina, “Italy vetoes 5G deal between Fastweb and China’s Huawei: sources.” *Reuters,* October 23, 2020, https://www.reuters.com/article/us-huawei-italy-5g-idUSKBN2782A5.
33. Supantha Mukherjee and Helena Soderpalm, “Sweden bans Huawei, ZTE from upcoming 5G networks,” *Reuters*, October 20, 2020, https://www.reuters.com/article/sweden-huawei-int/sweden-bans-huawei-zte-from-upcoming-5g-networks-idUSKBN2750WA.
34. Leo Kelion, “Huawei 5G kit must be removed from UK by 2027,” *BBC News*, July 14, 2020, https://www.bbc.com/news/technology-53403793.
35. Uwe Parpart and David Goldman, “Germany battles over Huawei’s 5G role,” *Asia Times*, October 7, 2020, https://asiatimes.com/2020/10/germany-battles-over-huaweis-5g-role/.
36. Amy Kazmin and Stephanie Findlay, “India moves to cut Huawei gear from telecoms network,” *Financial Review*, August 25, 2020, https://www.afr.com/world/asia/india-moves-to-cut-huawei-gear-from-telecoms-network-20200825-p55p6g#.
37. Sameer Yasir and Hari Kumar, “India bans 118 apps as Indian soldier is killed on disputed border,” *The New York Times*, September 2, 2020, https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html.
38. “EU-US: A new transatlantic agenda for global change,” https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279.
39. Srijan Shukla, “UK wants 5G alliance of 10 countries, including India, to avoid reliance on Chinese Huawei,” *ThePrint*, May 29, 2020, https://theprint.in/world/uk-wants-5g-alliance-of-10-countries-including-india-to-avoid-reliance-on-chinese-huawei/431735/.
40. Alan Tovey, “MPs want China, Russia barred from defence chain,” *The Telegraph*, February 1, 2021, https://www.telegraph.co.uk/business/2021/02/14/mps-want-china-russia-barred-defence-chain/.
41. Daniel Michaels and Valentina Pop, “China Faces European Obstacles as Some Countries Heed U.S. Pressure,” *The Wall Street Journal*, February 23, 2021, https://www.wsj.com/articles/china-faces-european-obstacles-as-some-countries-heed-u-s-pressure-11614088843?mod=djem10point.
42. “Joint Statement by the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), January 5, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.
43. Ericka Chickowski, “Next-Gen Supply Chain Attacks Surge 430%,” *DarkReading*, August 21, 2020, https://www.darkreading.com/application-security/next-gen-supply-chain-attacks-surge-430-/d/d-id/1338717.

NOTES

44. Matt Solomon, "Lessons Learned from the Global Year in Breach: Supply Chain Cybersecurity Risk is Swamping Businesses," *Security Boulevard,* April 24, 2021, https://securityboulevard.com/2021/04/lessons-learned-from-the-global-year-in-breach-supply-chain-cybersecurity-risk-is-swamping-businesses/.
45. Prak Chan Thul, "Cambodia adopts China-style internet gateway amid opposition crackdown," *Reuters*, February 17, 2021, https://www.reuters.com/article/amp/idUSKBN2AH1CZ.
46. Ashley Westerman, "To the dismay of free speech advocates, Vietnam rolls out controversial cyber law," *NPR*. January 1, 2019, https://www.npr.org/2019/01/01/681373274/to-the-dismay-of-free-speech-advocates-vietnam-rolls-out-controversial-cyber-law.
47. Patpicha Tanakasempipat, "Thailand passes internet security law decried as 'cyber martial law'," *Reuters.* February 28, 2019, https://www.reuters.com/article/us-thailand-cyber/thailand-passes-internet-security-law-decried-as-cyber-martial-law-idUSKCN1QH1OB.
48. Charles Rollet, "Ecuador's All-Seeing Eye is Made in China," *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.
49. Catalin Cimpanu, "Kazakhstan government is intercepting HTTPS traffic in its capital," ZDNet." December 6, 2020, https://www.zdnet.com/article/kazakhstan-government-is-intercepting-https-traffic-in-its-capital/.
50. "Targeted, Cut Off, and Left in the Dark," AccessNow, 2019 Report, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.
51. Isobel Asher Hamilton, "268 million people had their internet shut off by government-imposed blackouts in 2020, up 49% from 2019," Business Insider, https://www.businessinsider.com/government-internet-blackouts-human-rights-india-kashmir-coronavirus-2021-1.
52. Editorial Staff, "BCI Supply Chain Resilience Report 2019," *Continuity Insights*, November 7, 2019, https://continuityinsights.com/bci-supply-chain-resilience-report-2019/.
53. Adam Jacobson, "The Economic Costs of Government Internet Interruptions," *Risk Management Monitor*, May 7, 2019, https://www.riskmanagementmonitor.com/the-economic-costs-of-internet-interruptions/.
54. Chloe Taylor, "Government-led internet shutdowns cost the global economy $8 billion in 2019, research says," CNBC, January 8, 2020, https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html.
55. Isobel Asher Hamilton, Government-imposed internet blackouts cost the global economy $8 billion in 2019, and 2020 could be even worse," *Business Insider*, January 18, 2020, https://www.businessinsider.com/internet-shutdowns-cost-the-global-economy-8-billion-in-2019-2020-1.
56. Ian King, "Intel CEO's New Crusade Pits Investors Against U.S. Interests," *Bloomberg*, January 22, 2021, https://www.bloomberg.com/news/articles/2021-01-22/intel-ceo-s-new-crusade-pits-investors-against-u-s-interests.
57. Joe Miller, "Porsche rules out Chinese factory as it hails cachet of 'Made in Germany'," Financial Times, February 14, 2021, https://www.ft.com/content/d71660bf-ae2b-41b3-af99-1485b805c812.
58. "Democracies must team up to take on China in technosphere," *The Economist,* November 21, 2020, https://www.econom ist.com/briefing/2020/11/19/democracies-must-team-up-to-take-on-china-in-the-technosphere.
59. Bob Davis, "White House Weighs New Action Against Beijing," *The Wall Street Journal,* November 23, 2020, https://www.wsj.com/articles/white-house-weighs-new-action-against-beijing-11606138925.
60. "Australia demands China explain why it has been singled out on trade restrictions" *The Guardian*, November 22, 2020, https://www.theguardian.com/australia-news/2020/nov/22/australia-demands-china-explain-why-it-has-been-singled-out-on-trade-restrictions.
61. Rajiv Shah, "Ensuring a trusted 5G ecosystem of vendors and technology," *Australian Strategic Policy Institute*, September 17, 2020, https://www.aspi.org.au/report/ensuring-trusted-5g-ecosystem-vendors-and-technology,
62. "Australia spends $500,000 to strengthen tech ties with Quad allies amid China tension," *The Guardian*, November 23, 2020, https://www.theguardian.com/australia-news/2020/nov/23/australia-spends-500000-to-strengthen-tech-ties-with-quad-allies-amid-china-tension.
63. David Ignatius, "Biden's ambitious plan to push back against techno-autocracies," *The Washington Post*, February 11, 2021, https://www.washingtonpost.com/opinions/bidens-ambitious-plan-to-push-back-against-techno-autocracies/2021/02/11/2f2a358e-6cb6-11eb-9ead-673168d5b874_story.html.

NOTES

64. Joint Statement from Quad Leaders," September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/.
65. David Stilwell and Dan Negrea, "Wanted: Alliance Networks for a New Cold War." National Interest, March 28, 2021, https://nationalinterest.org/feature/wanted-alliance-networks-new-cold-war-181177.
66. Chaim Gartenberg, "The Biden administration is working to help address global semiconductor chip shortage," *The Verge*, February 11, 2021, https://www.theverge.com/2021/2/11/22278431/biden-administration-global-semiconductor-chip-shortage-executive-order..
67. "Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities," June 8, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/.
68. Russell Brandon, "It will cost $1.8 billion to pull Huawei and ZTE out of US networks, FCC says," The Verge, September 4, 2020, https://www.theverge.com/2020/9/4/21422939/huawei-zte-us-phone-networks-fcc-congress-reimbursement-cost.
69. Uwe Parpart and David Goldman, "Germany battles over Huawei's 5G role," *Asia Times*, October 7, 2020, https://asiatimes.com/2020/10/germany-battles-over-huaweis-5g-role/.
70. U.S. Department of Treasury, 2019, Enforcement Information, https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information. .
71. Statement of Commissioner Geoffrey Starks," February 17, 2021, https://docs.fcc.gov/public/attachments/DOC-370055A4.pdf.
72. Samantha Schwartz, "Technology's greatest supply chain challenge? Establishing trust, *Cybersecurity Dive*, January 21, 2021, https://www.cybersecuritydive.com/news/solarwinds-response-nation-state-threat/593239/. .
73. "US: Building a More Effective Strategy for ICt Supply Chain Security," *BSA Position Paper*, February 16, 2021, https://www.bsa.org/policy-filings/us-building-a-more-effective-strategy-for-ict-supply-chain-security.
74. Samuel Woodhams and Simon Migliano, "Big Tech Supporting Blacklisted Surveillance Companies," *TOP10VPN*, May 21, 2020, https://www.top10vpn.com/research/investigations/big-tech-supporting-blacklisted-surveillance-companies/.
75. Mara Hvistendahl, "How Oracle Sells Repression in China," The Intercept, February 18, 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.
76. "U.S. Chamber Releases In-Depth Analysis of U.S.-China Economic Relationship," February 17, 2021, https://www.uschamber.com/press-release/us-chamber-releases-depth-analysis-of-us-china-economic-relationship.
77. Jon Chesto, "Manufacturers provide lifelines during the pandemic, for their employees as well as front-line workers," *Boston Globe*, June 9, 2020, https://www.bostonglobe.com/2020/06/08/business/manufacturers-provide-lifelines-during-pandemic-their-employees-well-front-line-workers/.
78. Wombi Rose, "Two weeks of sleepless nights turn 3D card maker into PPE provider," *Lovepop*, May 13, 2020, https://www.lovepopcards.com/blogs/pop-up-cards/two-weeks-of-sleepless-nights-to-turn-3d-card-maker-into-ppe-provider. .
79. Sean O'Kane, "How GM and Ford Switched Out Pickup Trucks for Breathing Machines," *The Verge*, April 15, 2020, https://www.theverge.com/2020/4/15/21222219/general-motors-ventec-ventilators-ford-tesla-coronavirus-covid-19.

Socio-Technical-Economic Systems (STES) Unlearned Lessons

What Corrodes Cyber, Infects its Offspring: Unlearned Lessons for Emerging Technologies

Dr. Chris C. Demchak

Making the Self-Evident Obvious[1]

What infects the cyberspace societal substrate also infects its technological offspring. Whatever relies on the current shoddy, insecure cyberspace substrate inherits its vulnerabilities. This great silent unlearned lesson among technologists, promoters, government officials, and ignorant or optimistic users seems self-evident and yet is repeatedly unlearned. It would seem self-evident that, unless the underlying substrate is transformed to be securable, any new technology built on those insecure cyber foundations will, in turn, fall prey to the same assaults. That adversary and criminal campaigns to poison data, corrupt algorithms, and 'p0wn' development processes are fairly predictable is logically obvious for AI systems as well as quantum, robotics, autonomous systems, synthetic biology, and any other emerging technologies. They all rely on the highly corruptible, existing cyberspace substrate and inherit its attack surfaces in addition to new ones of their own.

This logic and lesson of inter-generational sharing of vulnerabilities is clearly not obvious to the bulk of the information technology (IT) community responsible for developing the programs, collating the data, or using the results, tools, and products in established or emerging technologies. Even the advanced and most respected policy schools feeding the top ranks of the national policy elite did not perceive the logic despite having the president of the US declare in 2009 that cybersecurity is "one of the most serious economic and national security challenges we face,"[2] As late as the mid-2010s, most major master's programs in public affairs, political policy, international relations, business administration, law, or criminal justice did not yet include cybersecurity courses (or even cybersecurity components as part of their existing curricula) for their students.[3]

All the ideas in this essay are solely those of the author, and do not reflect the positions or policies of the U.S. Government, U.S. Navy, or the U.S. Naval War College.

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

As further evidence of how little learning about computer vulnerabilities has penetrated the national zeitgeist, a myriad of revealed cyber-attacks over the past ten years has taken most of the past decade to spur broader and more concrete systemic action across the IT capital goods industry. For most of the past three decades, only occasional or niche admiration of this ubiquitous insecurity problem pockmarked the thinking across computer science professionals, Internet promoters, IT capital goods enterprises, and political decision-makers. Only recently have we seen the development of the "DevSecOps" (development security operations) concept across the information systems community, with the goal of securing software during its development.[4] However, it has yet to solidify as a defined set of basic processes embedded in the design, development, and implementation of new technology (software and hardware).[5]

Even further behind in learning this lesson are the various communities of emerging technologies. Especially noteworthy is artificial intelligence, arguably the most widely applied of the major emerging technologies. Although it has been around in either a software or an algorithmic form since the 1950s,[6] only since 2010[7] have some developers begun to warn about the cybersecurity threats to AI products. Moreover, only since 2017 – as though these vulnerabilities were something newly noticed and in need of explanation – has that warning become more vigorous.[8] Over the same period, however, according to one AI safety company's CEO, vulnerabilities have increased five thousand percent.[9]

The situation is only going to get worse, the longer the lesson about how a shoddy cyberspace parent infects its emerging technology offspring is ignored. *"Those attacks are going to become more and more pervasive, more and more prevalent, especially as [advanced battle management system] and [Joint All-Domain Command and Control] get implemented out into* *a wider context. The amount of data is going to explode beyond anybody's expectations. ... I'm talking about the sheer collection of that data and what that enables our adversaries to do and to think about."*[10] According to a recent Microsoft survey of machine learning developers, 25 of the 28 groups interviewed did not know how to secure their machine learning systems, making their security awareness and posture effectively zero.[11]

At the end of the day, the brave new world of emerging technologies will only be as secure as the highly insecure underlying substrate on which they are being built, in which they are being embedded, and through which they are expected to operate transparently, accurately, and resiliently. Until we collectively transform that substrate in order to secure it, though, our future with emerging technologies will be one of exquisite and inexplicable further failures and ceding technological dominance ground to adversaries able to manipulate key national systems. This equally self-evident future path is apparently also not obvious.

"NMPY" – Not My Problem Yet

Why emerging technology developers would put cybersecurity aside during their project creation is understandable. First, most AI developers have been trained as computer scientists or mathematicians or they have grown up in the IT capital goods communities.[12] Little to none of their training specifically focused on the inherent security complexity of the computer languages they know, the programs they run, or the products they make. Indeed, security for computer products in general is relegated to minimal efforts inserted late in the development process with after-market updates left to be someone else's problem.

Second, it is hard enough to get a new machine learning (ML) model to work at all and to gather all the data needed just to train it, let alone slow down its development to worry about what exploit might attack the model and/or its data once it is deployed. One analogy – although a weak one – might be that of designing a ground-breaking new kind of car engine. No producer wants to ask their engineers working on the engine to slow down development in order to first figure out what stresses the new marvel will put on the braking system or even how exactly the braking system will work in the final design. That problem is left to others to solve once the new engine actually works and provides the additional thrust, efficiency, or mileage that then undermines the current brake design. Similarly, the incentive is enormous to just get the ML model to do what was envisioned. For developers, worrying about someone or something later messing that up has long been considered a step too far.

Third, this lesson is tough to learn because of the inherent opacity of the product, even more difficult to disaggregate than the code of a classic computer program. The latter is largely readable by a human, but the model's operating neural networks – modern AI's machine learning workhorses – are not. Machine learning is so heavily dependent on complex structures of opaque computerized calculations. Leaving aside adversaries, the AI/ML models can perform poorly for a wide range of obscure reasons constituting the normal accidents of complex systems.[13] Intentional or accidental corruption of one or more of its three main development components – the tools, the models, and the data used to train the models – is exceptionally difficult to detect.[14]

Fourth, the inherent optimism of the computer science culture pushes against expecting the worst. Of course, it is recognized that at some point someone in the real world will connect the new AI product, new robot, or new autonomous system to old(er) networks, even if only for updates. Yet. this recognition does not invoke security concerns; indeed, AI and ML are usually characterized as separate from cybersecurity in casual discussion. Generally, the terms are connected with "and" as though they are two different topics, independent of each other. As Lt. Gen. Mary O'Brien, Air Force deputy chief of staff for intelligence, surveillance, reconnaissance, and cyber effects operations, recently noted: *"[t]there's an assumption that once we have the AI, we develop the algorithm, we've had the training data, you know, it's giving us whatever it is we want it to do, that there's no risk, that there's no threat."*[15]

While the Air Force is commonly assumed to be the most advanced US military service in terms of artificial intelligence,[16] Lt. Gen. O'Brien also noted that the service has no unit dedicated to defending the ML algorithms once they are deployed for use and called an officer suggesting the creation of such an AI red team a "maverick."[17] While this term was used with respect, If an officer need, to be a maverick to make the obvious connection that these newer systems will be intrinsically vulnerable, then the lesson of cybersecurity – so poorly and slowly learned in the parent field of computer science – has even less penetrated the more opaque world of AI/ML development.

The Peer Adversary Knows the Lesson, at Least as an Opportunity for Attacks

The time left to learn the lesson about cybered defense of AI/ML shortens daily as westernized democracies fall behind in having a skilled and well-educated workforce able to both develop and find ways to defend AI/ML systems. Aside from the sheer scale of the 5:1 advantage in the overall population compared to the US, China's strategic and well-funded dedication to technology dominance in the last half-century is paying off. Not only has the US' main peer adversary developed a commanding lead over the US in several emerging technologies, but it is also outpacing the US in the number of graduates in STEM subjects. China outspends and outgraduates the US in STEM graduates and Ph.D.'s.[18] There are more Chinese computer science graduates in a year than the US has graduated in all of its STEM programs.[19] Concerning AI, in particular, the US' top twenty accredited universities' Centers of Academic Excellence in Cyber Operations (CAE-CO) offer fewer AI/ML classes for their students than the equivalent eleven schools in China.[20]

Furthermore, China uses its centralized authority to mandate AI education in its high school curricula and requires AI companies to partner with schools and universities to help train students. Whereas the US federal approach is piecemeal, hampered by the Constitutional allocation of education sovereignty to individual states and even districts. Since 2018, the Chinese government approved at least 345 universities to offer an AI major – now the country's most popular – and at least 34 universities have launched their own AI institutes.[21] The US, by comparison, is experimenting with AI education curricula and industry partnership initiatives, but still in a piecemeal way that varies by state and places a heavier emphasis on computer science education.

Other emerging technologies such as quantum or advanced bio-engineering fare little better. At least for the developers and potential clients of those new and emerging technologies, the awareness exists that the new technology can be corrupted. Quantum computing, for example, is widely viewed as both a benefit to cybersecurity due to the difficulty of breaking its encryption or obtaining unauthorized decryption but also as a potential disaster for the currently dominant asymmetric, public-key encryption that could, in the near future, be made obsolete by quantum decryption.[22] The main adversary for consolidated democracies, China, has noted the connection between cyberspace and quantum or AI/ML or space. It is making massive strides in keeping with its scale and strategic coherence advantage, funding, mandating, and facilitating quantum research and production, along with its computer science, artificial intelligence, and other emerging technology initiatives. The chief adversary has learned the lesson, still just being admired by the democratic defenders.

*If the Apple Does Not Fall Far from the Tree – Learn to Transform the Tre*e

The consequences of not learning how to defend both the cyberspace substrate and its offspring, such as AI, can be dire in the future. While most emerging technology initiatives across consolidated democracies are waiting on lagging market forces to notice, care about, catch up with, and then act to defend cyber/AI systems and any other new technologies, a horde of AI-familiar students exit Chinese high schools and then college to transform their national socio-technical-economic system (STES) and their future prosperity. In the near-medium future, the US and its allies will face not only a tsunami of overwhelming cyber-attacks, which they will have to defend but will also experience vastly greater losses as their advanced and emerging technologies are stolen, corrupted, disrupted, or remotely controlled. The exponential growth of adversaries' skilled attackers, processes, and advanced technologies offers opportunities for more accidents, errors, and malicious interventions.

China also suffers from the same NMPY attitude among its developers of emerging technology. Still, China's leadership has already moved from problem admiration to action to protect its substrate and, by extension, its own development and use of emerging technologies. Certainly, the leadership has learned the lesson about the connection between poor underlying cybersecurity and the future prosperity and defense of the national STES. Its own expertise in cyber-attacks on other nations' cyberspace and emerging technologies indicates what could be done to China itself should the democratic states engage in the same cyber campaigns and mirror China's poor state behaviors in hacking. Fearing those reprisals or exploitation in return, the Chinese regime has created a National Cybersecurity Center to address the underlying insecurity of its cyberspace substrate with generous funding and government top-down authorities.[23]

One of its goals is to displace foreign technology, a process that could mean replicating shoddy existing technology with mirrored equivalents built in China and perhaps coded in native Mandarin. However, it is likely also to mean that, given the surge in the national development of computer science and related talent, this pursuit will generate at scale a bevy of discoveries and innovations. If so, Chinese computer science will transform its own national substrate into something more secure for the benefit of China alone, further ensuring the gap between its technological vigor and the digital security of the consolidated democracies.

Leaving this lesson unlearned is a major national security threat for the US and its allies if these numbers hold true in the future. "[B]y the year 2025 more money will be spent on artificial intelligence software and services than on infrastructure-as-a-service and platforms-as-a-service."[24] The race to incorporate artificial intelligence in the form of machine learning and reinforcement learning is showing a pattern of “adopt-before-securing” just like the race to computerize that engulfed the advanced economies in the early 2000s. That earlier wildly enthusiastic develop-and-promote era cemented technological flaws and insecurities deeply within the cyberspace substrate – the same underlayment that threatens these new emerging technologies. The difference now is that a major authoritarian nation is rushing in with the intent to dominate the technology globally. Even if it is rushed and somewhat slipshod, China’s progress in replacing foreign technology with indigenous means that the fragmented democracies will be left with emerging technologies more vulnerable to compromise. At the same time, they will find it harder to defend against the more technologically literate, large state. Over time, they will also fall further behind in their ability to reciprocate attacks by disrupting the adversary’s increasingly different and likely more defensible cyber substrate.

Action is needed now, and it must be collective action across the consolidated democracies to increase their scale and the pace of transformation of the underlying cyberspace substrate and the emerging technologies themselves.[25] Unfortunately, there is no automatic win for the westernized “likeminded” nations in the future if this lesson remains unlearned. Whatever is done by either authoritarian adversaries or consolidated democracies to transform their underlying vulnerable cyberspace into a more securable substrate will increase the chances of defensible operations for their technological advances emerging now and in the future. The only question is whether the consolidated democracies or the huge rising authoritarian peer power learns or benefits from this lesson sooner. The quicker student wins the better future, and the future of democracy as a desirable model for a prosperous, advanced, and secure society rests on the outcome.

NOTES

1. A seminal Berkeley professor of complexity, technology, and society, Dr. Todd R. LaPorte, commented once that often the most significant role of social scientists is to make the self-evident obvious to those who were not paying close attention. Personal discussion.
2. Barack Obama, White House Press Conference: Remarks by the President on Securing our Nation's Cyber Infrastructure, US Government (Washington DC, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.
3. Francesca Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," Pell Center for International Relations and Public Policies, March 2013, https://salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf.
4. Håvard Myrbakken and Ricardo Colomo-Palacios, "DevSecOps: A multivocal literature review," paper presented at the International Conference on Software Process Improvement and Capability Determination, https://www.researchgate.net/profile/Havard-Myrbakken/publication/319633880_DevSecOps_A_Multivocal_Literature_Review/links/59da4c47a6fdcc2aad12a134/DevSecOps-A-Multivocal-Literature-Review.pdf 2017.
5. Runfeng Mao et al., "Preliminary findings about devsecops from grey literature," paper presented at the 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS), https://qrs20.techconf.org/QRS2020_FULL/pdfs/QRS2020-4LGdOos7NAbR8M2s6S6ezE/891300a450/891300a450.pdf 2020.
6. Melanie Mitchell, Artificial intelligence: A guide for thinking humans (New York: Picador, 2019), https://melaniemitchell.me/aibook/.
7. Pavel Laskov and Richard Lippmann, "Machine learning in adversarial environments," Machine Learning 81, no. 2 (2010), https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.375.4564&rep=rep1&type=pdf.
8. For an example, see the OpenAI blog found at https://openai.com/blog/adversarial-example-research/.
9. Patrick Tucker, "US Needs to Defend Its Artificial Intelligence Better, Says Pentagon No. 2 – AI safety is often overlooked in the private sector, but Deputy Secretary Kathleen Hicks wants the Defense Department to lead a cultural change," Defense One, June 22, 2021, https://www.defenseone.com/technology/2021/06/us-needs-defend-its-artificial-intelligence-better-says-pentagon-no-2/174876/.
10. Patrick Tucker, "Vulnerabilities May Slow Air Force's Adoption of Artificial Intelligence – More data on the battlefield means a wider attack surface, something the Defense Department has yet to prepare for, experts say," Defense One, September 23, 2021, https://www.defenseone.com/threats/2021/09/vulnerabilities-may-slow-air-forces-adoption-artificial-intelligence/185592/.
11. Dr. Hyrum Anderson at Microsoft, Enigma 2021 talk, https://www.youtube.com/watch?v=RWx_DitGF7A.
12. Term originally used by John Mallery, CEO of Work Factors Group in multiple presentations 2010-2020, Cambridge.
13. Zachary Arnold and Helen Toner, AI Accidents: An Emerging Threat – What Could Happen and What to Do, Georgetown University Center for Security and Emerging Technology CSET (July 2021), https://cset.georgetown.edu/publication/ai-accidents-an-emerging-threat/.
14. Andrew Lohn, Poison in the Well: Securing the Shared Resources of Machine Learning, Georgetown University Center for Security and Emerging Technology (CSET), June 2021, https://cset.georgetown.edu/publication/poison-in-the-well/.
15. Billy Mitchell, "As Air Force adopts AI, it must also defend it, intelligence chief says," FedScoop, September 22, 2021, https://www.fedscoop.com/air-force-artificial-intelligence-algorithm-defend-intelligence-chief-mary-obrien/.
16. Author personal conversations within the US AI defense community.
17. Mitchell, "As Air Force adopts AI, it must also defend it, intelligence chief says."
18. Remco Zwetsloot et al., China Is Fast Outpacing U.S. STEM PhD Growth, Georgetown University CSET, August 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/.
19. Steven Overly and Melissa Heikkila, "China wants to dominate AI. The U.S. and Europe need each other to tame it," Politico, March 2, 2021, https://www.politico.com/news/2021/03/02/china-us-europe-ai-regulation-472120.
20. Dahlia Peterson, Kayla Goode, and Diana Gehlhaus, AI Education in China and the United States — A Comparative Assessment, Georgetown University Center for Security and Emerging Technology,September 2021, https://cset.georgetown.edu/publication/ai-education-in-china-and-the-united-states/.
21. Peterson, Goode, and Gehlhaus, AI Education in China and the United States – A Comparative Assessment.

NOTES

22. Neha Sharma and Ramkumar Ketti Ramachandran, "Emerging Trends of Quantum Computing: The Emerging Trends of Quantum Computing Towards Data Security and Key Management," Archives of Computational Methods in Engineering, April 28, 2021.
23. Dakota Cary, China's National Cybersecurity Center – A Base for Military-Civil Fusion in the Cyber Domain, CSET Georgetown University Center for Security and Emerging Technology CSET,July 2021, https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.
24. Simon Sharwood, "AI to be bigger than IaaS and PaaS combined by 2025 – $500bn a year to be spent on electro-brain and supporting tech vs $400bn on cloud infrastructure," The Register, August 6, 2021, https://www.theregister.com/2021/08/06/idc_ai_paas_iaas_predictions/.
25. Chris C. Demchak, "Cyber Competition to Cybered Conflict," eds, Emily Goldman, Jacqueline Schneider, and Michael Warner, Ten Years In: Implementing New Strategic Approaches to Cyberspace (Naval War College Press, The Newport Papers, 2020, https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.

Extracting Unlearned Lessons from Past Poor Choices lest They be Learned the Hard Way in the Future

Dan Geer

Unlearned lessons are those insights missed from a past situation. When we do not learn from experiences, we continue to make the same decisions in similar situations. In the case of the United States, unlearned lessons undermine the future security and prosperity of democracies. The results of unlearned lessons can be the individual's free choice, but others, including some facing us now, heavily burden the future with the collective history of other prior choices. More volatile times face open societies globally. As Nassim Taleb observes, when the tails of a probability distribution get fatter, the predictable becomes a function of the distribution's extreme values and only those extreme values.[1] In multiple publications, Taleb argues that the world is "undergoing a switch between continuous low-grade volatility to a process moving by jumps, with less and less variations outside of jumps."[2] The faster the rate of systems change, the heavier become those tails, due mostly to the growth of unrecognized interdependence between the moving parts. In the statistical analysis of systems, if one is uncertain about the tails of the data, then one is uncertain about the mean as well. Yet, the faster the rate of systems change, the heavier become those tails, due mostly to the growth of unrecognized interdependence between the moving parts, and thus the less useful for learning are their means. Such a situation requires the prudent person to plan for maximal damage scenarios, not for most probable scenarios, and to ensure that the choices they make along the way offer reasonable and secure alternatives when the worst scenarios emerge.

Rather than exploring one or two broad unlearned lessons, as in other articles in this publication, this essay presents a series of questions in an arbitrary order whose answers could lead to different possible futures. These questions, and the choices made

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Dan Geer, Senior Fellow, In-Q-Tel. Milestones: The X Window System and Kerberos (1988), the first information security consulting firm on Wall Street (1992), convenor of the first academic conference on mobile computing (1993), convenor of the first academic conference on electronic commerce (1995), the "Risk Management is Where the Money Is" speech that changed the focus of security (1998), the Presidency of USENIX Association (2000), the first call for the eclipse of authentication by accountability (2002), principal author of "Cyberinsecurity: The Cost of Monopoly" (2003), co-founder of SecurityMetrics.Org (2004), convener of MetriCon (2006-present), author of "Economics & Strategies of Data Security" (2008), and author of "Cybersecurity & National Policy" (2010). Creator of the Index of Cyber Security (2011) and the Cyber Security Decision Market (2012). Lifetime Achievement Award, USENIX Association, (2011). Expert for NSA Science of Security award (2013-present). Cybersecurity Hall of Fame (2016) and ISSA Hall of Fame (2019). Testified five times before Congress.

in answering them, are not commonly addressed in the broader literature. This essay intends to capture choices in national cybersecurity of which we seem unaware, yet which have great steering power that, ten years from now, will seem obvious in retrospect. By then, some of the choices that follow below will have already been made, choices that are expensive to reverse in either dollars or clock-ticks. These questions are neither mutually exclusive nor collectively exhaustive, but each marks a fork in the road and a lesson yet to be learned about the complexity of our society, choices, and futures. Each question is chosen to illustrate an extant fork in the road to the future.

SURVEYING UNLEARNED LESSONS IN UNAPPRECIATED PAST FORKS IN THE ROAD

Automation: Over time, does automation help defense or offense more?

If the answer over time is offense, then cybersecurity becomes more like nuclear deterrence, including that there are few precision weapons and that enforceable treaties are essential to our survival. If the answer is defense, then we should turn to algorithms to do what we cannot otherwise do, that is, to protect us from other algorithms.[3]

Connectivity without Management: How much do we allow self-modifying decision-making to free-run?

The Berkeley SWARM lab says that there will be 1,000 radios per person on earth within five years, while Pete Diamandis (X Prize) says within 15 years, there will be 10,000 sensors per person. That scale exceeds manageability, so that technology must just be allowed to free-run. Yet, if that free-running is self-modifying, then it will be unable to be evaluated for trustworthiness. The choice is to what extent we will pair free-running with self-modifying cybersecurity systems, and the challenge then will be by what mechanisms will we make that choice stick.

***Metrics as Policy Driver: Do we steer by Mean Time Between Failure (MTBF) or Mean Time To Repair (MTTR) in Cybersecurity?*[4]**

Choosing Mean Time Between Failure (MTBF) as the core driver of cybersecurity assumes that vulnerabilities are sparse, not dense. If they are sparse, then the treasure spent finding them is well-spent so long as we are not deploying new vulnerabilities faster than we are eliminating old ones. If they are dense, then any treasure spent finding them is more than wasted; it is disinformation. Suppose we cannot answer whether vulnerabilities are sparse or dense. In that case, a Mean Time To Repair (MTTR) of zero (instant recovery) is more consistent with planning for maximal damage scenarios. The lesson under these circumstances is that the paramount security engineering design goal becomes no silent failure – not no failure but no *silent* failure – one cannot mitigate what one does not recognize is happening.

Embedded Systems: Do we require devices to either be updatable or have a finite lifetime?

A remote management interface is required for updatability, but such an interface is itself a potential risk should it be cracked.[5] Yet, doing without remote updates risks having devices that are immortal and unfixable unless a finite lifetime is purposefully designed in. Enforcement of either mandate—that of a remotely fixable or pre-limited lifetime—is an expressly government issue, and enforcement means culpability for those who fail to implement the one or the other. But the choice then becomes hinged on how that culpability is defined and enforced. One lesson to note is that devices that are unlocatable after deployment are a special case where remote updates are not possible; these devices must have limited lifetimes.

Composability: Since non-composability—where secure A plus secure B does not make a secure A+B—is common, how is research directed?

Composability is both a research and commercial opportunity that allows cybersecurity to aggregate as the sum of secure parts. This is the inherent security-in-the-limit question for the supply chain model. Within the narrow domain of just input parsers, for example, hostile data input is so very often the mechanism by which exploit is triggered.[6] Composable parsing would yield much general benefit, and not just for cybersecurity if research were to resolve the mechanisms of its creation or at least the detection of cybersecurity non-composability in critical supply chains. With some encouragement, DARPA has become interested in looking at composability, but more attention is needed.

Reproducible Buildability: Do we mandate that the software supply chain be checkable, or should the buyer absorb all the risk?

Olav Lysne has shown that, in the limit, electronic equipment from untrusted vendors cannot be verified.[7] If we choose not to let the buyer absorb all the risk, then the fallback choice is to introduce process requirements, requiring merchants of digital goods to retain the ability to recreate those digital goods exactly as deployed. This obligation requires that the build environment is preserved in working detail. A nascent, international effort on "reproducible builds" is making technical progress but more support is needed to make this choice a reality.[8]

Abandonment: Every kind of property save software can be seized in the public interest if and when abandoned; how do we define and remedy software abandonment going forward?

When a supplier declares that a software product is “no longer supported,” the software should be considered abandoned, thus triggering some legal seizure or collection process. The most straightforward remedy would be to open-source abandoned codebases. Another would be to seize cryptographic keys of signal value, such as those of a certifying authority that goes out of business. The nascent Microsoft/GitHub arctic repository of code on which "we the people" depend is an example answer of serious preservation, but it is not a legal answer applicable across national systems. The lessons of abandoned and unsupported software in the wild already are well demonstrated, making this question another in which choices here channel the future and have yet to be learned.[9]

Attribution: Do we geocode the Internet by fiat or keep arguing about attribution?

Nationally, a public safety argument drove the requirement to geocode mobile phones in real-time. The sanctity of all financial services already starts with “know your customer,” including from where they normally connect to the Internet. Whereas intercontinental ballistic missiles have a visible flight path and a limited number of launch-capable governments, yet offensive software has neither. Would geocoding the Internet offer a simple attribution resolution? The Westphalian principle is clear for state responsibility; if packets are allowed to exit a nation’s territory, then that country must have strict liability for them regardless of any actual negligence or intent to harm on that nation’s part. Despite concerns with adversaries’ engaging in false flag campaigns by routing traffic through other nations, the greater harm lies in not choosing to at least know the origins of traffic entering and exiting nations.[10]

Prioritization: Does continuous machine learning require prioritizing integrity over confidentiality?

Confidentiality has long been first among equals within the classic triad of confidentiality, integrity, and availability (CIA). As data collection grows in breadth and depth, and as data-driven algorithms take broad control of the physical world with the corruption of inputs among the larger threats, must not data integrity take priority over availability and availability take priority over confidentiality? If this is the moment of overturning that prior order, then much different design regimes must be deployed, including, but not limited to, robust data chain of custody regimes uninfluenceable by single points of failure.[11]

Data Mitigation: What mitigation, if any, can be enforced for data loss immortalized in immutable storage (such as blockchains)?

Inherent to blockchain design, the insertion of bad things onto blockchains has no reversal mechanism, no "undo" is available. Do those who manage blockchains without a deletion mechanism inherit strict liability for the consequences of the blockchain's misuse as the publisher of illicit, inaccurate, or harmful goods? If they do not, then who is liable and for how long?[12] Do democratic societies proscribe certain information from being put in immutable storage?

Namelessness: Do we require resolvable names for some classes of services?

At present, name resolution is the double-entry bookkeeping of the internet. In this process, if A claims this specific name and URL address pair are connected, then B can verify A's claim with third parties. In the absence of verifiable names, however, how does anyone verify to whom they are connected? If names are not required, a wide range of subordinate questions whose answers have considerable impact emerge because one side of the verifying bookkeeping is now missing. Should a (nameless) address be permitted to be baked into code and, if so, where? Are software updating engines supposed to reach out to devices that have only a network address and no name? What happens if an endpoint that is asked to accept an update has no name to check? Do we need to develop a two-class liability system and/or duty to support name verification, one for checkable name-to-address pairs versus one for un-named addresses? Will internal firewalls now have to include a key-centric, rather than a name-centric, PKI? Does a MAC address or a UUID-in-ROM distinguish keys in a nameless world and thus offer an alternative to an identity-based PKI tied to hardware? Either way, these choices have implications for a range of internet security management, especially as to whether the key-management job is going to be harder or easier absent names.[13] What would be the risk interaction of a nameless internet with an IPv6 world too big to enumerate, especially when IPv6 protocols inherently allow address hopping and multi-homing, challenging existing security regimes?

Interrogability: Does one accept dependence on black-box algorithms, and if so, to what extent?

Machine learning from noisy datasets delivers equations where coefficient values have no inferential meaning and are likely to have the fragility that comes from over-fitting. Algorithmic decision-making is being increasingly challenged by new rules and regulations around the world that are attempting to increase transparency and limit disfavored outcomes. Article 15 (and others) in the European Union's General Data Protection Regulation (GDPR), for example, creates a right to challenge any algorithmic decision by asking "why?", which cannot be answered by an uninterrogable algorithm.[14] Does this create a new variety of "informed consent" when a medical algorithm says what must be done but cannot explain why? And so what, exactly, does "informed" in "informed consent" then mean? Similarly, military users will likely be reluctant to permit algorithms to apply deadly force if those algorithms cannot explain themselves in the vernacular. At what level of criticality do we require interrogability prior to legal deployment?

Insurance: What is the definition of force majeure in cybersecurity?

As Mondelez v Zurich and Merck v Allianz/AIG show, what is force majeure in cybersecurity may be judiciable. Since many instances of attack have no immediately identifiable attacker, how will this work out? Has the burden of proof for payout shifted from proving "I was harmed" to proving "I was harmed, and I can prove that I was the actual target"? Besides that, how will risk pooling—the very premise of insurance—proceed in the future? At some level of personalization, there is nothing left with which to pool.[15]

Entity scale: Are cloud computing suppliers critical infrastructure?

The very smallest companies and the very biggest companies are safer if they do their computing on-premises, whereas middling companies are safer if they do their computing in the cloud.[16] In a target-rich world, the smaller organizations do not draw as many attacks, while the bigger ones have the dollars to invest in stronger cybersecurity and corner the talent market. The middle-sized organizations are, therefore, all but obliged to have somebody else mind the cookstove. So, does it then follow that cloud computing suppliers have the duties of a critical infrastructure provider? Do we replicate the regulatory structure surrounding Systemically Important Financial Institutions (SIFI) for computing entities that are not "too big to fail" but rather "too interconnected to fail"? What is the policy analog for a cloud provider to SIFI's capital adequacy requirements or any of the rest of the financial stress-testing regime? Since the bulk of regulation for financial services is the accumulation of past failures, shall we just wait for cloud failures of sufficiently serious kinds to occur and then design appropriate regulations?

Failure as design: When a functionality is a security failure by-design, who pays the price?

Repeatedly, we feign surprise when an ICT product or service is found to have design failures. As an engineer would say, what might be possible and consistent with the paradigm of risk tolerance is that no system may fail silently. In a sense, that is what data breach laws assume—that breaches will happen no matter what and that the proper response is remediation and notification of affected parties. If users consider notification adequate mitigation, then this type of law does create a form of security as the surprise is followed by its mitigation. Any regulation in this area would include performance standards for a latency of cleanup steps, like notification.

Moreover, as a Verizon Data Breach Report noted, 3/4 of all data losses are discovered by unrelated third parties, and whether data breaches are preponderantly insider attacks or outsider attacks depends on the definition of an "insider." If "insider" means "on the payroll," then insider attacks are not the most important issue. If, however, insiders include folks on the payroll, plus employees of the organization's partners or vendors who have as-of-right access to that company's infrastructure, plus employees of those in its supply chain, then the majority of data losses are insider attacks.[17]

Ownership: Should the beneficial owner of software also own its risks?

Today, suppliers claim ownership for the software they sell and license to users, yet via the pervasively unreadable End User License Agreement, they disclaim all responsibility for what they say they own. This contradiction now applies to countless mélanges of hardware and software from the biggest to the smallest products. This can either continue toward its logical conclusion, that users own nothing and have no recourse, or it can be steered (at least in democratic countries) toward some form of software liability. To do that, new constructions of strict liability and merchantability are necessary, especially considering self-modifying software where the copy a user has may well be unique.[18] This fork in the road demonstrates, more than others, that does not make a clear decision in this instance is equivalent to having made a decision. A plague of lobbyists can be expected to join the fray here.

Truth: What are the trust anchors we now need?

While the common use of the term "trust anchor" refers to the self-signed certificate at the head of a specific cryptographic hierarchy, here it is intended in a policy and societal sense. As Malcolm Gladwell has persuasively argued, civil society only works if its members can safely default to trust in dealing with each other.[19] As the digitalization of society proceeds, the presence of cyber risk makes defaulting to trust look increasingly naive. What divergence effects do you get if, among humans, you more or less have to default to trust, whereas in bitspace, you more or less have to default to mistrust or, as it is now commonly referred to, adopt a "zero trust" policy?

Sovereignty: Is it more prudent for the US to ban certain technology (e.g., Huawei) or to do what it takes to have technical leadership?

The intersection of patents and standards, and the coercion or protection applied to intellectual property distinguishes an authoritarian system versus a democratic system. The global suppliers will not take sides out of unpressured patriotism. For small countries, the choice is mostly whose technology to adopt and thus what side-effects to endure. For great cyber powers, the choice is whether to do what it takes to win the technology race. Furthermore, democratic nations do things with allies, not to them.

Balkanization: Should the trade in network and security gear mimic the trade in arms, that is to say, that you only buy or sell within your allies or region?

This question concerns whether all sellers become holding companies so that, for example, the Apple-China team does one thing while the Apple-EU team does another. A government official saying "your government needs you to do us a favor" is probably a seller issue more than a buyer issue. Even if there is no nation-state pressure on a supplier to install an exploitable flaw, that "do us a favor" can take the form "you are forbidden to fix the following flaw." Or is nation-state the wrong granularity here? Some Google security engineers say they only trust Google-manufactured phones as other manufacturers modify the Android software and may install other software as part of the base install. A few major banks no longer buy application software, they write their own. As cyber sovereignty spreads, it could come to require that one runs only code that one or one's allies directly wrote.

Strategy: What strategy is most cost-effective for cybersecurity: cost-efficiency or cost-effectiveness?

Cost/benefit analysis is useless and wasteful for cybersecurity; what matters is cost-effectiveness. The fork in this road is to prove that a body of code implements its specifications and no more than its specifications or to embrace a moving target defense. Code proofing, the first option, is a—if not the—gold standard, but it is also difficult to do. After a successful proof is in hand, an organization must adopt strict change control to protect its investment. The second option is moving target defense, which is comparatively easy and may work well enough to diminish today's strategic asymmetry that favors attackers over defenders. However, it also guarantees that how any fielded instance of code actually works on any endpoint is not obvious. It requires an intermediary to explain the process. Brutal change control – the first option – damps down the rate of change, which may be an acceptable price to pay for stamping out cyber exploits and other vulnerabilities. Moving target defense does not care if there is a new set of vulnerabilities with every revision, which may be an acceptable price to pay for stamping out cyber exploits and other vulnerabilities.[20]

Taking either path is a choice supported by results obtained by serious scientists; it is also one of those choices that are expensive in either dollars or clock-ticks to later reverse.

Analog fallback: If a state of security is the absence of unmitigable surprise, what is the mitigation for an irrecoverable software fault?

Of all the forks or choices enumerated in this article, this one is the most telling choice. Optimality and efficiency work counter to robustness and resilience. Complexity hides interdependence, and unacknowledged interdependence is the source of black swan events. The benefits of digitalization are not transitive, but the risks are. Because single points of failure require militarization wherever they underlie gross societal dependencies, frank minimization of the number of such single points of failure is a national security obligation. Cascade failure ignited by random faults is quenched by redundancy, whereas cascade failure ignited by sentient opponents is exacerbated by redundancy. Therefore, the preservation of uncorrelated operational mechanisms is likewise a national security obligation. Those uncorrelated operational mechanisms are the analog alternative.

The ability to operate in the absence of the Internet and all that it delivers requires retaining the pre-digital analog realm is crucial. It does not share common-mode failures with the digital realm, nor does analog create pathways to cascade failure. To retain the analog realm, it must be updated, used, and exercised, and not left sitting on some societal shelf hoping that it still works when some emergency demands that it work. As a current example, consider the regulatory and public policy debate ongoing in Sweden on how to retain a sufficient baseload of cash processing such that the mechanisms needed to use cash do not disappear, even if society is moving toward a cashless system.[21] Sweden is now choosing whether to make cash processing a critical infrastructure and to do so by regulation. Mere economics will otherwise create a singleton risk of society-wide failure.

In short, the intervention is to require, by force of law, that those who choose to opt-out of the digital world do not do so at the price of moving back to the 15th century, that accommodating those who opt-out is precisely and uniquely how to maintain a baseload for nearly all the essential components of our daily living. Perhaps never before and never again will national security and individual freedom jointly share a call for the same initiative at the same time. The active preservation of the analog option must come soon if it is to have the cost-effectiveness of preserving fully amortized infrastructure and not the sky-high costs of recreating it under emergency conditions.

THE UNDERLYING UNLEARNED LESSON: KEEP ANALOG OPTION HEALTHY AND AVAILABLE

As mentioned at the outset of this essay, the prudent person should plan for maximal damage scenarios, not for the most probable scenarios, and avoid creating feelings of safety that are unwarranted.[22] Most important ideas are not exciting. Most exciting ideas are not important. Not every problem has a good solution. Every solution has side effects. To learn the unlearned lessons of the past, it is best to have a prudence doctrine and anticipate possible future losses but not future gains.[23]

While change is inevitable, undirected change does not produce some steady upslope at 8% grade; instead, the course of undirected change naturally traces through periods of quietude interrupted by bursts of self-reinforcing change. The evolutionary biologist Stephen Jay Gould called this phenomenon a “punctuated equilibrium.”[24] By this author’s count, there have been three “equilibrium punctuations” to date. The first was circa 1995: a TCP/IP stack appeared as a freebie in Microsoft Windows, exposing an unhardened operating system to the world, a change that birthed the cybersecurity industry. Second, circa 2005: cybered opponents changed from braggarts to professionals, a critical change because while braggarts may share their tools, professionals hold them closely. The professional's ever-increasing stockpile of software exploits is why zero-days have come to dominate risk. Third, circa 2015: blind automation of flaw finding—which was a DARPA Cyber Grand Challenge intended to help defense—is becoming a central tool in the attackers' kit and is perhaps the ultimate proof that all security technology is dual-use. Looming is a fourth punctuation, possibly circa 2025, as a wide variety of developments in emerging technology and geopolitics converge. The choices being made now will be as consequential as any that have been made before.

At the end of the day, ordered liberty depends on putting a speed limit on irrevocable change. We cannot be passive.

NOTES

1. Pasquale Cirillo and Nassim Nicholas Taleb, "What are the chances of a third world war?" *Significance* 13, no. 2 (2015).
2. Nassim Nicholas Taleb Pasquale Cirillo, "On the Statistical Properties and Tail Risk of Violent Conflicts," *Physica A: Statistical Mechanics and its Applications,* no. 429 (2016), https://arxiv.org/abs/1505.04722.
3. Https://spw18.langsec.org/slides/Vanegue-AEGC-5-year-perspective.pdf.
4. Https:// www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197.
5. https:// tools.ietf.org/html/rfc791.
6. https:// langsec.org.
7. Olav Lysne, *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment?* (Springer Nature, 2018).
8. https:// reproducible-builds.org.
9. http:// geer.tinho.net/ieee/ieee.sp.geer.1307.pdf.
10. http:// geer.tinho.net/ieee/ieee.sp.geer.1707.pdf.
11. http:// geer.tinho.net/ieee/ieee.sp.geer.1801.pdf.
12. https:// news.bitcoin.com/a-brief-history-of-hidden-messages-in-the-bitcoin-blockchain.
13. http:// geer.tinho.net/fgm/fgm.geer.1812.pdf.
14. https:// www.clarip.com/data-privacy/gdpr-article-15.
15. www.bloomberg.com/news/features/2019-12-03/merck-cyberattack- s-1-3-billion-question-was-it-an-act-of-war
16. geer.tinho.net/fgm/fgm.geer.1909.pdf; and geer.tinho.net/fgm/fgm.geer.1412.pdf.
17. http://geer.tinho.net/ieee/ieee.sp.geer.1911.pdf, http://geer.tinho.net/fgm/fgm.geer.2006.pdf; http://geer.tinho.net/fgm/fgm.geer.2012.pdf; http:// geer.tinho.net/fgm/fgm.geer.1906.pdf.
18. The End of Ownership, Perzanowski & Schultz, MIT, 2019, and http://geer.tinho.net/ieee/ieee.sp.geer.1907.pdf.
19. Talking to Strangers, Gladwell, Hachette Book Group, 2019.
20. https://www.ll.mit.edu/sites/default/files/page/doc/2018-05/22_1_8_Okhravi.pdf.
21. https://www.ft.com/content/c4ea6fb3-6262-4426-9503-05391f0e523a.
22. http://geer.tinho.net/geer.mindthesec.16ix20.txt.
23. https://www.hoover.org/research/rubicon.
24. Niles Eldredge & S.J. Gould, "Punctuated equilibria: an alternative to phyletic gradualism" In T.J.M. Schopf, ed., Models in Paleobiology. San Francisco: Freeman Cooper, 82-115 (1972); Stephen Jay Gould and Stephen Jay Gould, *Punctuated equilibrium* (Harvard University Press, 2009).

Four Questions Indicating Unlearned Lessons Concerning Future Military Digital Systems and Fleet Design

Sam J. Tangredi, Ph.D.
CAPT, USN (Ret.)

The US military knows well that it is fully engaged in ongoing 'peacetime' cybered conflict against state and nonstate actors intending to harm the US and its allies and partners.[1] This enduring conflict is driven by various motives and takes myriad forms, ranging from ransomware attacks and theft of technical intellectual property to what is, in effect, cyber privateering and piracy. Various issues afflict the cyberspace substrate and extend deep into the socio-technical-economic system (STES) of modern Western democracies. Given the grievous damage that could be done, these vulnerabilities—many self-inflicted—are astounding.

Yet, to some extent, the US military (and perhaps its allies as well) perceives its forces and systems to be partially immune (at least internally) from these 'civilian' vulnerabilities since it has 'secure' communications, networks kept apart from the public internet, and air gaps between weapons systems and outside digital threats. But is this accurate?

Four Questions in Search of Answers and Lessons Yet to be Learned

Previous discussions in this volume prompt four questions concerning the vulnerabilities of military systems. DoD, at least in part, is addressing some of these questions. However, the scope of the vulnerabilities in the civilian socio-technical-economic system (STES), which resources our military, seem so vast as to require multiple answers (and efforts to mitigate) for each concern. The first three questions apply to all US military services, and the final question applies specifically to the U.S. Navy.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Dr. Tangredi is the Leidos Chair of Future Warfare Studies, Director of the Institute for Future Warfare Studies, and Professor of National, Naval and Maritime Strategy in the Center for Naval Warfare Studies of the U.S. Naval War College. He has wide experience as a strategic planner and director of strategic planning teams. His books include *AI at War: How Big Data, Artificial Intelligence*, and *Machine Learning Are Changing Naval Warfare*, edited with George Galdorisi (Naval Institute Press, 2021), and *Anti-Access Warfare: Countering A2/AD Strategies* (Naval Institute Press, 2013). Dr. Tangredi is a retired U.S. Navy Captain who held command at sea.

1. To **what extent is the tradeoff between security and efficiency or convenience**—the latter having rendered STES vulnerable—**creeping into the military** via adoption of current commercial business practices (e.g., just-in-time delivery), or from the small and inorganic threats that STES routinely encounters in 'peacetime' systems operations and maintenance?
2. Is the combination of threats such that **a reserve force of less digitally-dependent (or completely analog) systems** is advisable to ensure the force and fleet continuity in the highly cybered and electromagnetic spectrum-contested combat environment that will characterize any future conflict against a technological near-peer?
3. Will the contested cyberspace and electromagnetic environment **drive DoD toward autonomous systems that** operate under the concept of mission command because **we will not be able to keep the human-in-the-loop**?
4. Are the myriad digital threats such that the **U.S. Navy cannot successfully achieve the distributed maritime operations (DMO) concept** on which it expects to anchor its future fleet design? (Note: Fleet design encompasses both fleet structure and operational doctrine.)

The brief scope of this essay does not allow for answers to these questions; thorough discussion of each would require its own volume. This essay focuses on Naval lessons yet to be learned, and leaves the first three questions for the reader to ponder.

Cyber Vulnerabilities and Fleet Structure

One unlearned lesson is whether the U.S. Navy should retain less-digitized ships, aircraft, and other naval systems as an operational reserve. Arguments advanced by other experts in this collection make it unclear whether even the most highly digitized/cybered systems can themselves survive on the modern battlefield in a conflict between technological near-peers in which cyberspace and the electromagnetic spectrum is contested. Each new capability brings new vulnerabilities—new avenues and opportunities for penetration and compromise. The greater the dependency on wireless communications within the system itself, the greater the need for (a) communications with remote offboard sensors or controls and (b) effective real time assessment of equipment status, given the greater exposure to cyber/electromagnetic penetration of those communication loops.[2]

All defense acquisition programs must now have a cyber security protection plan to mitigate cybered threats to program management, systems design, and supply chain, in order to mitigate a potential penetration of initial system acquisition. Even in the cases where these plans are in place—and many are, in reality, just risk assessments—they cannot guarantee protection throughout the lifecycle of a system that requires periodic updates, installation of new combat systems, and added commercial systems, such as low-cost navigation radars, etc.

System survivability is largely a function of two variables: vulnerability, and resilience, or bounce back. The closer a system must operate in proximity to an opponent's means to conduct the fight in the electromagnetic spectrum, the more important these factors become. Determining conclusively whether analog systems might, in fact, be more survivable in a cyberspace and electromagnetic spectrum contested environment is long overdue.

Distributed Maritime Operations - Driven to Complete Autonomy?

Another unlearned lesson is that cyber vulnerabilities could channel those operational concepts that are workable. For a critical example, cyber insecurities may prevent the U.S. Navy from achieving its goal of *distributed maritime operations* (DMO). To avoid compromising its networks via the penetration of its long-range wireless communications, may require the Navy to retain its current battle group concept of operations to allow ships unfettered communications via local networks utilizing line-of-sight UHF signals or through retransmission nodes such as drone aircraft. Without some assurance of communications continuity under battle conditions, the overall distributed network could conceivably collapse into local networks—basically independent battlegroups.

Local commanders may also be driven to authorizing more autonomy with less human-in-the-loop control or even minimizing use of key capabilities because of untrusted systems that are vulnerable to adversary meddling. Over the past several years, the Navy has presented several fleet structure plans to the Secretary of Defense and Congress that call for a larger fleet made up of a mix of manned and unmanned ships (as well as manned and unmanned aircraft).[4] This is despite insufficient open discussion of the vulnerabilities that unmanned systems will face in the real world of cybered conflict and electromagnetic warfare. How will humans retain control over these systems in a hacked environment? Manned systems will also face considerable vulnerabilities, but presumably, with crews trained to defend the critical networks and override automated control that has been electronically captured by the enemy.

How can the Navy (and DoD overall) ensure the security – and hence trustworthiness – of the hundreds of thousands of lines of code in these unmanned systems created by contracted programmers, perhaps using programs with unknown vulnerabilities? Continual inspection of code (with the added costs that requires)? How will intrusion, misdirection, or disruption be prevented in the wireless networks that provide both the sensor and commands information to the unmanned systems? These signals can be encrypted, but there are well-known difficulties in maintaining these systems' currency under the measures/counter-measures nature of warfare.

These vulnerabilities may drive the operational commanders to increase autonomy in their local area. In this circumstance, the unmanned half of the fleet will need to be to less under the direct control of 'humans in the loop' given the need to act quickly without communications prone to adversaries can disrupt or intercept. To counter command or other remote cyber intrusions, may require operations under principles of "mission command" that operate independently, with or without return to relay what they accomplished.[5]

Another aspect of this unlearned lesson is that the full implications of cyber vulnerabilities in unmanned systems are likely apparent only after they are deployed and fail operationally. Mitigating the threat and learning the lesson in advance, would require DoD policy changes,[6]and doctrinal changes in current naval warfare planning centered on fleet Maritime Operations Centers (MOCs)—perhaps proactively accepting the realities of unrestricted warfare in localized settings in anticipation of cyber-related command failures. There may be technical fixes to attempt—perhaps burst transmissions relayed via satellite to and from the autonomous platforms. However, as contributors to this volume argue, every technical fix brings its own technical vulnerabilities.[7] If the enemy can geolocate the burst transmissions, the autonomous systems become easier targets. Some argue that these vulnerabilities may be mitigated by developments in artificial intelligence (AI) systems. Yet some in this issue note that AI is linked tightly to cyber capabilities, and brings its vulnerabilities as well. Even new levels and intensity of deception need to be anticipated with rising dependence on AI.[8]

Little Hope for an Equal Field/Sea of Combat

Many contributors to this volume suggest methods by which the socio-technical-economic systems (STES) of Western democracies can be hardened and made more resilient.[9] Whether these methods are ever adopted is not a choice within the purview of the militaries of consolidated democracies. What does fall within that purview is an examination of their systems, procedures, doctrine, and force designs to seriously and routinely determine vulnerabilities that could be exploited in a conflict with a technological near-peer like China. Without doing so, there is little hope for an equal field or sea of combat. A good start in learning the lessons neglected so far would be for the Navy to grapple with and answer the four questions identified.

NOTES

1. Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age " *Strategic Studies Quarterly* 5, no. 1 (March 1, 2011).
2. There are proposals for methods to determine whether military aircraft have been hacked. See for example Marcus Weisgerber, "New Tech Aims to Tell Pilots When Their Plane Has Been Hacked," *Defense One* (web), October 4, 2019, https://www.defenseone.com/business/2019/10/new-app-tells-pilots-when-their-plane-has-been-hacked/160378/.
3. Defense Acquisition University, "Chapter 9 – Program Protection," *Defense Acquisition Guidebook,* September 22, 2020, https://www.dau.edu/guidebooks/shared%20documents/chapter%209%20program%20protection.pdf
4. On the latest iteration, see Megan Eckstein, "Navy releases long-range shipbuilding plan that drops emphasis on 355 ships, lays out fleet design priorities," *Defense News,* June 17, 2021, https://www.defensenews.com/naval/2021/06/17/navy-releases-long-range-shipbuilding-plan-that-drops-emphasis-on-355-ships-lays-out-fleet-design-priorities/.
5. See Robert C. Rubel, "Mission Command in a Future Naval Combat Environment," *Naval War College Review* 71, no. 2 (Spring 2018), pp. 109-122, https://digital-commons.usnwc.edu/nwc-review/vol71/iss2/8/.
6. Captain George Galdorisi, USN (Ret.), "Keeping Humans in the Loop," United States Naval Institute *Proceedings,* 141, no. 2 (February 2015), pp. 36-41, https://www.usni.org/magazines/proceedings/2015/february/keeping-humans-loop.
7. Giles Peeters, "A Short Burst Data Capability," *MilsatMagazine* (web), April 2013, http://www.milsatmagazine.com/story.php?number=2121128035.
8. See Sam J. Tangredi, "Sun Tzu Versus AI: Why Artificial Intelligence Can Fail in Great Power Conflict," United States Naval Institute *Proceedings,* 147, no. 5 (May 2021), pp. 20-25, https://www.usni.org/magazines/proceedings/2021/may/sun-tzu-versus-ai-why-artificial-intelligence-can-fail-great-power.
9. Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).

Content as Infrastructure: The Unlearned Lesson about Cyber Security and Information Integrity

Sean Kanuck

Why Content Matters

Informational content is just beginning to be properly considered as an urgent infrastructure security concern in addition to the physical integrity and functionality of the computers and telecommunications networks that enable the transmission of such content. The 2016 and 2020 presidential elections in the United States (US) raised awareness about disinformation campaigns and greatly increased both public and private sector efforts to combat foreign influence operations. But the importance of informational content goes far beyond its potential cognitive impact on human actors, such as voters. Automated industrial control systems (ICS) and Internet of Things (IoT) devices can be adversely impacted, or even maliciously manipulated, as well. In a world of heightened reliance on artificial intelligence (AI) and/or machine learning (ML) algorithms – which require large volumes of training data – content becomes part of the infrastructure, because each datum that is processed contributes to the future functionality of the algorithm. AI/ML algorithms that are trained on or receive disinformation inputs will yield imperfect outputs.

Privately owned smartphones and IoT devices are among the many endpoints that will be dependent on AI and fifth generation telecommunications networks (5G); therefore, they – and their human users – will remain highly susceptible to the effects of false data inputs. Moreover, the compounding effects that an AI algorithm creates from any disinformation that it ingests become a genuine concern in the context of IoT, for a single error can then create cascading effects over time and across physical space. One false positive in a computer vision program could lead to the misclassification of many other objects

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Sean Kanuck is CEO of the strategic consulting firm EXEDEC and an Affiliate of Stanford University's Center for International Security and Cooperation (CISAC). Previously, Sean served as the first U.S. National Intelligence Officer for Cyber Issues from 2011 to 2016 after a decade of experience in the CIA's Information Operations Center, including both analytic and field assignments. He was also appointed Chair of the Research Advisory Group for the Global Commission on the Stability of Cyberspace and Director of Cyber, Space and Future Conflict at the International Institute for Strategic Studies.

Sean holds degrees from Harvard University (J.D.; A.B. in Government & Philosophy), the London School of Economics (M.Sc. in International Relations), and the University of Oslo (LL.M. in Public International Law). He teaches graduate courses at George Washington University's Elliott School of International Affairs and George Mason University's Law School on artificial intelligence, national security law, and ethics.

in the future. False negatives introduced into a medical screening algorithm could impair the identification of similar life-threatening conditions in other patients. In the context of national security, automated sensing platforms, or analytic algorithms processing their data streams, that were compromised in one instance could either fail to warn of imminent danger on another occasion (i.e., false negative) or inappropriately escalate hostilities (i.e., false positive).

Whether decision makers are human beings (e.g., political leaders, military commanders, corporate executives, investors, air traffic controllers, healthcare workers, etc.) or computer programs (e.g., lethal autonomous weapons systems (LAWS), nodes on an energy grid, high-speed trading algorithms, self-driving cars, etc.), the accuracy of information is paramount for it to be actionable and trustworthy. It is also important to distinguish between the nuanced concepts of "accuracy" and "veracity" for information. The accuracy – or integrity – of information means that the data in question accurately reflects its desired or correctly inputted form; however, that does not mean such data is inherently true. Veracity, on the other hand, refers to the ultimate truth or falsehood of the data (especially as it may relate to predicting future events).

For example, a medical report could accurately enumerate the fears of a paranoid schizophrenic patient, even though such fears were ill-founded (and therefore not veracious). Similarly, a military situation report could inform a commanding officer of accurate observations, but which were actually activities designed by the adversary to mislead and deceive observing forces regarding its true intentions or maneuvers. More hypothetical scenarios will put the need for human oversight and collateral analysis into full perspective. Conceivably, a telecommunications intercept of a phone call or email could accurately report the content of that message even if the sender of the message either inadvertently or intentionally transmitted false information.

In that case, the data would meet the accuracy parameter, but the information would not meet the veracity assessment. One can also imagine a contrarian investor who bets on market positions against the "perceived wisdom" of the majority. She would want to accurately know what her counterparts believed, even if she did not place value in the veracity of their assessments. Depending on the application, veracity may be desired, but accuracy of data is always required.

United States Cyber Doctrine

When the United States Government (USG) began publishing its cyberspace strategic doctrine in the 1990s, it used different terminology and a much more holistic approach than it did in the early 2000s. The Department of Defense (DoD) issued Joint Pub 3-13.1 entitled "Joint Doctrine for Command and Control Warfare (C2W)" on February 7, 1996.[1] That publication presciently contextualized the actionable value of informational content:

> Information warfare (IW) capitalizes on the growing sophistication, connectivity, and reliance on information technology. The ultimate target of IW is the information dependent process, whether human or automated.[2]

Joint Pub 3-13.1 (1996) further described the military's role in the conflict over the value of information as follows:

> Command and control warfare (C2W) is an application of IW in military operations and employs various techniques and technologies to attack or protect a specific target set — command and control (C2). C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions.[3]

Then, the DoD issued Joint Pub 3-13 entitled "Joint Doctrine for Information Operations" on 9 October 1998,[4] which defined offensive and defensive information operations (IO) as follows:

> Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives .... Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems.[5]

In the 1990s, the DoD's emphasis was clearly on protecting the value of information and impairing or manipulating the ability of adversarial military commanders to effectively make sound decisions based on the data they were receiving. Moreover, the full range of IO and IW was understood to strategically include all elements of society that depended on modern ICTs. In his 2002 article entitled "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age" for the U.S. Naval War College volume on "Computer Network Attack and International Law," Professor Daniel

Kuehl from the National Defense University wrote:

> The final major development shaping the new geostrategic context is the increasing reliance on computerized networks for the control and operation of key infrastructures in advanced societies. The growing reliance on these systems for the control and functioning of an increasingly large segment of the infrastructures on which we depend for economic, social, political, and even military strength is both a boon and vulnerability.[6]

In the two decades that followed the terrorist attacks on September 11, 2001, the USG and DoD took a decided turn towards a physical infrastructure security approach. Protection of physical assets – rather than informational assets – became the primary consideration and policy focus. "Homeland security" and "critical infrastructure protection" were promoted as the buzzwords for defending American interests against a new type of non-sovereign enemy that conducted sensational acts of physical violence and material destruction.

By June of 2018, the DoD's Joint Publication 3-12, entitled "Cyberspace Operations," reflected that conceptual shift to focusing on cyberspace as a vehicle (or means) for physical effect, rather than the information itself as the strategic end:

> Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. ... Relationship with the Physical Domains. Cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains.[7]

The focus on cyberspace as a fifth "domain" of warfighting furthered DoD's comparison to a physical realm and distracted from the essential and abstract qualities that made IO strategically significant. By 2018, the DoD had also reached an inflection point in its strategy for engaging in cyber operations. After the revocation of President Obama's Presidential Policy Directive for cyber operations (PPD-20) by President Trump,[8] the door was open for DoD to take a more leading policy role, and its publications announced a new doctrine for persistent, tactical engagement with adversaries in cyberspace.[9] Even in light of foreign disinformation campaigns and influence operations[10] the USG sought to disable the physical and/or virtual cyber capabilities of its adversaries in lieu of engaging them in robust information warfare (IW) per se. That distinction would be akin to using terrestrial military forces to prevent an enemy's air force from taking to the sky rather than developing one's own expertise in aerial combat.

Largely owing to its commitment to liberal democracy and freedom of expression, as embodied in the First Amendment to the United States Constitution, the USG is not inclined to perpetrate widespread disinformation campaigns. That reticence to participate in rampant IW as a modern means of force projection and coercive influence is also apparent from the diplomatic posture taken by USG representatives at United Nations (UN) working groups.[11]

Russian Information Security Doctrine

In marked contrast to the DoD's publications and USG submissions to the UN in recent decades, the Russian Federation has consistently highlighted the strategic significance of "information confrontation" from at least 2000.[12] In fact, Russia prefers the term "ICT" (i.e., information communication technologies) over "cyber" for that very reason. For the Kremlin, cyberspace is just a new technical means to enable national propaganda objectives that long predate the Internet, smartphones, or social media.

Russia's 2015 National Security Strategy specifically identifies "intensifying confrontation in the global information arena" as one of four key trends in international relations.[13] Moreover, Russia's 2016 Information Security Doctrine, clearly states that the "information sphere has a crucial role to play in the implementation of the strategic national priorities of the Russian Federation" and specifies several strategic objectives, including: (a) countervailing information and psychological actions; (b) suppressing … activity detrimental to the national security of the Russian Federation; and (c) neutralizing the information impact intended to erode Russia's traditional moral and spiritual values.[14]

In its 2011 document entitled "Conceptual Views Regarding Activities of the Armed Forces of the Russian Federation in the Information Space," the Russian government defined the role of its military to include:

> To maintain the forces and means for ensuring the information security in constant readiness for repulsing the threats of military and political character in the information space … The formation of the necessary public opinion implies its corresponding orientation and mobilization; it provides an opportunity to create in the global information space a climate promoting the limitation of the possibility for the perpetration by the organizers of the conflict of any further escalation steps.[15]

These strategic concepts have been formulated into an actionable hybrid warfare doctrine that is often (and perhaps erroneously) attributed to the Russian General Valery Gerasimov.[16]

Thus, there should be no surprise that Russia has pursued IO as an effective means of exerting coercive (as in the case of Ukraine) and meddling (as in the cases of the US and France) information operations through the strategic use of social media and disinformation. Cyberspace has provided a very effective platform for the prosecution of geographically distanced military operations aimed at destabilizing foreign governments and delegitimizing democratic institutions.

China's Military Doctrine

While China's publicly available documents are less explicit – and in many cases less bellicose – than those of either Russia or the US, China's military re-organization certainly conveys its strategic perspective. The formation of the Strategic Support Force (SSF) in 2015 has co-located the People's Liberation Army (PLA) units for cyber, space, and electronic warfare.[17] This new branch will have the ability to leverage a wide range of military assets for IO objectives and pursue more integrated operations to challenge or undermine information integrity on a global level.

China's diplomatic approaches at the United Nations (UN) also underscore Beijing's policy desire to avoid formal recognition of cyber warfare with physical effects under international humanitarian law without also addressing psychological effects.[18] Rather, China has approached the issue of defending cyber infrastructures as one that is inextricably linked to regulating publicly available information. Through the Shanghai Cooperation Organisation, Beijing joined Moscow in promoting an international code of conduct for cyberspace which focuses on information security vice cyber security.[19] The authoritarian leadership in China – as in Russia – is keenly aware of the political and strategic military value of controlling informational content both within and beyond its sovereign jurisdiction.

Back to the Future

The United States ushered in a new era of strategic thinking in the 1990s and then neglected it, only for its adversaries to more fully develop their own doctrines based on the same principles. Ironically, the United States and its allies are now returning to those earlier ideas as well as learning from adversarial doctrines and force structures. For example, four years after the formation of China's SSF, President Trump established the United States Space Force.[20] Beginning in 2015, the US Intelligence Community has formally highlighted the integrity of information with its potential impact on critical infrastructures (including IoT devices and AI algorithms) as a top national security concern.[21]

The last five years of DoD strategic thinking have also seen additional attention paid to the importance of information integrity in addition to the protection of physical assets for cyberspace. In particular, the June 2016 Strategy for Operations in the Information Environment (IE)[22] identifies a much more expansive end state objective: "through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations."[23] Further, the strategy clearly articulates the ultimate goal of impacting not only the content of information, but also the beliefs and perceptions of decision makers.

> Within the IE, the United States can expect challenges across three interrelated dimensions: the physical, composed of command and control systems, and the supporting infrastructure that enables individuals and organizations to create information-related effects; the informational, composed of the content

> itself, including the manner by which it is collected, processed, stored, disseminated, and protected; and the cognitive, composed of the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information. Effects in the physical and informational dimensions of the IE ultimately register an impact in the human cognitive dimension, making it the central object of operations in the IE.[24]

That strategy was followed by a Joint Concept for Operating in the Information Environment in July 2018,[25] which elaborates on the cognitive dimension.[26]

US and UK doctrinal thinking about cyber conflict and IO is also coming full circle, albeit under the new moniker of "cyber electromagnetic activity" or "CEMA". The UK Ministry of Defence's Joint Doctrine Note 1/18 from February 2018, entitled "Cyber and Electromagnetic Activities," summarizes its approach as follows:

> CEMA must address the longstanding challenges of acquiring, using and integrating information with physical actions to create the desired effect. In addition, information and the systems which create, collect, manage and exploit this information, are critical to successful conflict outcomes. The need for CEMA coordination, coherent with a full spectrum approach and mission assurance, has escalated in recent years because of the sheer volume of information, the ease of access to it and the increasing means by which it can be exploited.[27]

Re-Learning the Importance of Information Integrity

It appears now that the US is catching up to its previous self, China, and Russia on the doctrinal front, and must consider the way forward. Information integrity is essential to all aspects of modern societies. The 2011 Canadian federal election witnessed one party intentionally misinform the opposing party's supporters about changes to polling locations.[28] The Syrian Electronic Army's hack of the Associated Press's Twitter account and issuance of a false tweet about President Obama's wellbeing in 2013 caused a massive redistribution of wealth in the US financial markets.[29] In India, fake news propagated via social media has repeatedly been the impetus for sectarian violence and mass migrations.[30]

Each of these cases demonstrates how inaccurate data undermines the value of information, impairs the reliability of information sources, and/or erodes public trust and confidence. To maintain critical infrastructures in today's world, one must build resiliency not only of physical installations, but also of information resources. The mastery of the Russian GRU's interference in the US presidential elections[31] was that the operations willfully remained below the commonly accepted threshold of "threat or use of force"[32] because they indirectly caused American voters to cast valid – but albeit possibly misguided – ballots. Had a foreign power directly manipulated the actual polling results or used physical coercion, rather than psychological manipulation to affect voters, then the USG certainly would have taken a more profound response.

The preceding examples reflect the manipulation of human actors or decision makers, yet disinformation can be equally, if not more efficacious, when found in automated algorithms. In our increasingly networked society of "smart" (and inherently vulnerable) devices, AI is making more and more decisions for humans. The ability to misinform sensors, or manipulate infrastructure nodes, could have serious, cascading effects. Information operations against ICS controllers – as has occurred in the Iranian nuclear facilities – could destabilize public energy grids. The driverless cars and data-rich roads of the newly envisioned smart cities could lead to transportation nightmares and even loss of life if those AI algorithms do not operate correctly.

Content as Infrastructure

This article has argued that the USG's temporary turn away from its original strategic concept for cyber security (which fully valued the integrity of information) was deleterious. Only by conceiving the accuracy of data as a critical infrastructure element can we build genuine resilience. Errors, mistakes, misinformation, and disinformation can no longer be viewed as mere inputs that can be corrected later if needed. It may seem counterintuitive, but informational content must be viewed as infrastructure itself – not just data that is processed on infrastructure. The two can no longer be considered as indistinguishable. Content matters just as much as the systems used to transmit that content.

CONCLUSION

Recent experiences with foreign efforts to influence democratic elections through cyber hacks and social media campaigns as well as competing accounts regarding the origin, propagation, and mitigation of the COVID-19 pandemic have irreversibly shifted US strategic thinking to devote much more attention to informational content in addition to physical infrastructure protection. This is a very good and necessary development. We must appreciate that our infrastructure comprises informational assets as well as physical assets, just as ICT networks are composed of both hardware and software. Unfortunately, by losing sight of our own strategic thinking, the US was ill-prepared to address the activities of other nations that exploited our own doctrinal publications. That missed lesson permitted serious transgressions against our civic institutions, public trust, and economic well-being during the last five years. Hopefully, the lesson learned will be more enduring this time around.

NOTES

1. Available at JP 3_13_1 Joint Doctrine Command and Control Warfare (C2W) (iwar.org.uk).
2. See JP 3-13, Introduction, v.
3. See JP3-13, Introduction, v.
4. Daniel T Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," *International Law Studies* 76, no. 1 (2002), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils.
5. Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," viii.
6. Kuehl, "Information operations, information warfare, and computer network attack: Their relationship to national security in the information age," 42.
7. JP 3-12, Cyberspace Operations, 8 June 2018 (jcs.mil), vii.
8. Mack DeGeurin, "US Silently Enters New Age of Cyberwarfare," *New York Magazine*, September, 2018, http://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html.
9. U.S. Cyber Command USCC, Cyber Command Vision Statement, (https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf 2018).
10. Michael N Schmitt, "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chi. J. Int'l L.* 19 (2018).
11. Dennis Broeders, "The (im) possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment," *Journal of Cyber Policy* (2021), https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1916976.
12. See Putin’s 2000 information security doctrine. Łukasz Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016," *Studia z Dziejów Rosji i Europy Środkowo-Wschodniej* 52, no. 3 (2017).
13. See discussion of the 2015 strategy. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
14. See the 2016 doctrine. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
15. See the 2011 document. Dryblak, "The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016."
16. Eugene Rumer, *The Primakov (Not Gerasimov) Doctrine in Action - the Return of Global Russia*, Carnegie Endowment for International Peace (June 5, 2019), https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.
17. Elsa B Kania and John K Costello, "The Strategic Support Force and the Future of Chinese Information Operations," The *Cyber Defense Review 3*, no. 1 (2018), https://www.jstor.org/stable/pdf/26427379.pdf.
18. Kimberly Hsu and Craig Murray, *China and international law in cyberspace* (US-China Economic and Security Review Commission, 2014), https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.
19. Timothy Farnsworth, "China and Russia submit cyber proposal," *Arms Control Today* 41, no. 9 (2011).
20. Kaitlyn Johnson, "Space Force or Space Corps?," *The Center for Strategic and International Studies* (June 2019), https://www.csis.org/analysis/space-force-or-space-corps.
21. ODNI, Worldwide Threat Assessment of the US Intelligence Community, February 26, 2015, 3, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf, ODNI, Worldwide Threat Assessment of the US Intelligence Community, February 9, 2016, 1-2, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
22. Office of the Secretary of Defense DOD, DoD Strategy for Operations in the IE, (DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf 2016).
23. DOD, Short DoD Strategy for Operations in the IE, 2.
24. DOD, Short DoD Strategy for Operations in the IE, 3.

NOTES

25. Office of the Secretary of Defense DOD, Joint Concept for Operating in the Information Environment (JCOIE), (https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf 2018).
26. DOD, Short Joint Concept for Operating in the Information Environment (JCOIE), 2-3.
27. JDN 1/18, Cyber and Electromagnetic Activities (publishing.service.gov.uk), section 1.2
28. Staff Canadian Press, "Keys facts and timeline of events surrounding the [2011] robocalls scandal," *CBS News*, August 14 2014, https://www.cbc.ca/news/politics/key-facts-in-canada-s-robocalls-controversy-1.2736659.
29. Patti Domm, "False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked," *CNBC*, April 23 2013, https://www.cnbc.com/id/100646197.
30. India blames mass exodus on Pakistan groups | Asia| An in-depth look at news from across the continent | DW | 20.08.2012.
31. Robert S. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," (2019).
32. UN Charter Article 2(4).

Unlearned Lessons from the First Cybered Conflict Decade – BGP Hijacks Continue

Prof. Yuval Shavitt
Dr. Chris C. Demchak

INTRODUCTION

Unlearned lessons are those where the harm, attack methods, or malicious tools are demonstrated publicly and yet neglected by those who need to respond or better plan for future attacks. By 2010, reports of network traffic hijack attacks – called here Internet Protocol (IP) or Border Gateway Protocol (BGP) hijacks – had already surfaced. Most notably publicized was the China Telecom IP hijack attack in that year where 15% of the global Internet traffic was rerouted or "hijacked" through servers in China.[1] While the scale of this original event has been debated, there is little doubt that throughout the following decade, attacks of this kind continued. Eight years later, in 2018, we reported on China Telecom using its otherwise seemingly innocent network servers to reroute (or hijack) Internet traffic through China at its will. At the time, the company had 10 "points of presence" (PoPs, locations where a company's routing equipment is located) in North America, each strategically located and available to hijack or divert network traffic through China from North America.[2] The 2018 paper drew significant attention to the problem by the general public (through popular media outlets), the cybersecurity and research communities, and various stakeholders in western nations' governments, and yet the lesson is still unlearned by many of the same nations currently being victimized by China Telecom illicit activity and other BGP hijacks.

This essay discusses what has changed in the few years since the 2018 paper was published. Several interesting developments occurred in the last decade that suggest awareness is increasing but that the lessons are being learned too slowly and are still too fragmented across nations. Three years later, in 2021, we can report that China Telecom is still hijacking traffic using its global presence in Europe, Asia, and Africa. Major developments over the decade include three major observations.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Prof. Yuval Shavitt is Professor of Electrical Engineering at Tel Aviv University. Before joining Tel Aviv University, he worked for four years at the Networking Center of Bell Labs, Holmdel, NJ. He has published seminal papers in the fields of caching, routing, IP hijack attacks, and network measurements. In 2004, he founded the DIMES project for mapping the Internet infrastructure using thousands of lightweight software agents, which revolutionized the field of Internet measurement and mapping. Data gathered by DIMES was used by academicians worldwide. In 2014 he established BGProtect, a company that uses the DIMES approach to protect nations and large organizations against IP hijack attacks and provide network infrastructure threat intelligence.

1. Despite increased awareness of network operators and the networking research community regarding the risks of IP hijack attacks, the levels of adoption of means to make IP hijack attacks harder to carry out are still insufficient to declare this lesson learned.
2. The scale of the unfettered global expansion of large Chinese Internet service providers has made IP hijack execution somewhat easier and IP hijack detection harder worldwide.
3. Largely in North America and a narrow set of allies, an increased awareness among policymakers and other national leaders about Chinese-linked BGP attacks has led to enhanced efforts to use regulation to limit the use of Chinese telecommunication equipment and activities in critical national infrastructure, but many other states still welcome the overly generous and seemingly innocuous low-bids by Chinese vendors.

And the ‘game’ is still afoot. While the 2018 paper provides more detail on how the BGP hijacks occurred, it is helpful to reiterate a few details. The Internet is a global system of interconnected computer networks that push data to each other. Continuously, millions of streams of Internet traffic are guided from one node of a network through another and another, each possibly part of a different network, to the final destination node indicated by the published Border Gateway Protocol (BGP) routing tables. These intervening networks are, for routing purposes, called “autonomous systems” (AS) and are given unique numbers (AS Numbers, or ASNs) that are used to build the global BGP routing table. The tables themselves are constructed by the ASs self-reporting on what nodes they connect. During regular routing of Internet traffic, each AS announces its readiness to receive traffic and passes it along to neighbors by posting that information in BGP. With this information, the networks that are part of the Internet build their routing tables, which are used by each AS to send traffic from its internal customers on to others – in short, to anyone. IP hijack attacks are attacks where Internet traffic between the original sender and the destination is forced to travel along a set of intervening networks and nodes that include nefarious networks making copies of or alterations to the transiting Internet packets.

It is in the buried and often technical details of routing lists of ASs and transmission times that one finds small deviations or, changes in routes for nonaccidental periods of time. These deviations are often buried in the routes so that inattentive senders or recipients are not alerted. The traffic may arrive at its final destination a bit delayed, but in the meantime, it has been pushed unnecessarily through other nodes capable of making a quick copy of everything that transits through their location. Since the traffic eventually is received, it is and has been easy for either party (sender or receiver) or their network operators, to notice that critical information meant only for selected parties may be accumulating in someone else's database for decryption and use later.

For example, Figure 1 depicts routes from a recent deflection event in Europe. For about 10 minutes, traffic from hundreds of small networks worldwide (but mostly in Europe) was routed to COLT Telecommunications in West Europe via the TransTelecom's PoP in Moscow, Russia. TransTelecom was used by COLT to accept traffic from Russia and Central Asia. During the deflection event, COLT routes that were announced by TransTelecom were picked up by Russian Akado Telecom (previously known as Comcor) from Inetcom, a local Moscow provider. Akado Telecom then announced the routes to its many peers and, as a result, worldwide traffic (mostly from W. Europe) started traversing Moscow. The number of networks routing through TransTelecom during this deflection event increased sevenfold. The fact that only small networks were af-

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

fected by this deflection is unusual. This oddity suggested that larger networks, which would be more visible in the BGP monitoring tools, were not receiving these route announcements on purpose. The game can be quite subtle if the adversary is trying to operate unnoticed.

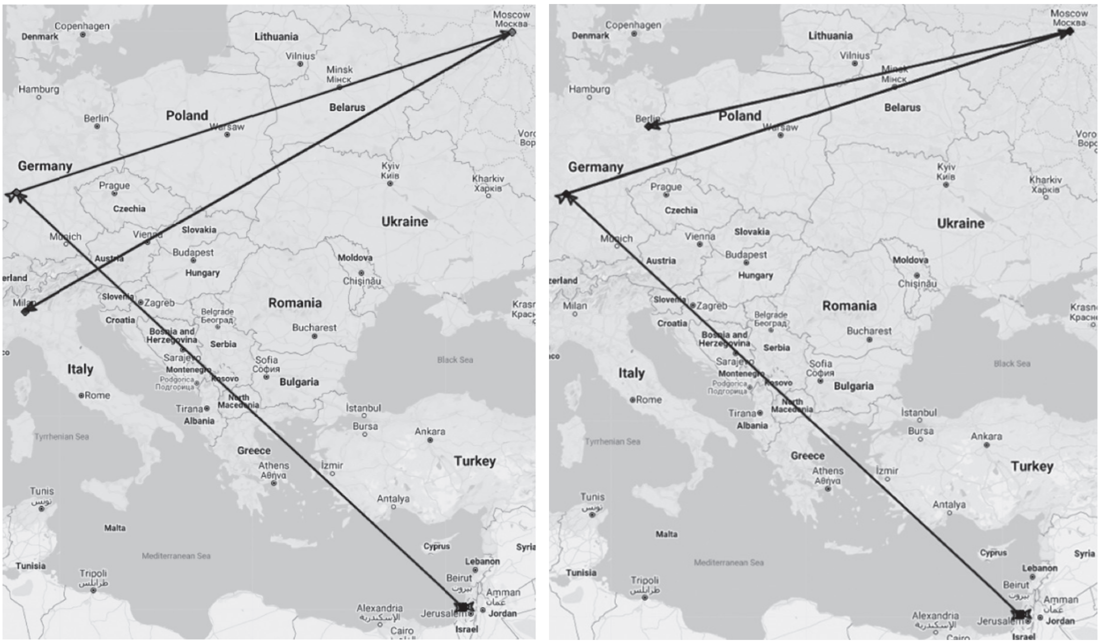


Figure 1: Two route examples from a 10-minute deflection of traffic towards COLT networks in West Europe via Moscow. The event occurred on March 7th, 2021, and affected traffic from hundreds of small networks around the world.

The Technology Sector Wakes Up – but Lessons Learned Lag Behind

By the late 2010s, there was increased awareness among network operators and the networking research community at risk about possible IP hijack attacks. The increase in the number of IP hijack attacks made "BGP hijack" a more familiar term that had emerged from obscurity to be known among technologists. In a survey conducted in 2017 among 75 network operators, over 90% of the surveyed operators claimed to be knowledgeable about BGP hijacking and how it happens. Yet, 41% reported that their organization had been a victim of a BGP hijack attack, and over half of the attacks lasted longer than an hour. A quarter lasted longer than a day, enabling a considerable amount of data to pass through unintended nodes in networks.[3]

As a result, there was also a reported increase in the adoption of means to make IP hijack attacks at least harder to carry out. The greater awareness of hijacking events led also to greater adoption of some operation norms by Internet service providers (ISPs). Until recently, one common way to hijack Internet traffic and reroute it to a block of IP addresses (an Address Prefix, or AP) was for the hijacking AS (Autonomous System or node in the network) to announce ownership of a particular AP using BGP. Since BGP was originally designed with no underlying security concerns, there is no intrinsic way in BGP to prevent any network on the Internet from announcing ownership of any AP regardless of its real owner. Over the years, large ISPs had adopted various means to verify that their customer networks do not announce APs that they are not allowed to announce. This verification, however, is not standardized and has been implemented inconsistently among network providers.

Some solutions have emerged but are still not consistently employed or standardized in processes or regulations. One promising standard – the Resource Public Key Infrastructure (RPKI), also known as Resource Certification, designed by the Internet Engineering Task Force (IETF) earlier on and available by 2011, was intended to solve the AP ownership verification, or in RPKI jargon, the Route Origin Authorization(ROA) in a standard way.[4] When using this standard, a distributed database allows each AP owner to communicate who is allowed to announce its address space. Since AP announcements carry the entire path to the AP, one can easily verify that the intended AS (namely the destination network) at the end of the route is legitimate.

Nonetheless, RPKI adoption has been irritatingly slow for most of the past decade. Momentum picked up significantly around 2017,[5] but recent statistics by the U.S. National Institute of Standards and Technology (NIST) show that only about one-third of the APs have valid RPKI entries.[6] Indeed, recent reports demonstrate that using RPKI improves the filtering of invalid route announcements.[7] However, it should be noted that RPKI protects against only one type of hijack attack (origin attacks), and it is not a comprehensive solution to the general problem of IP hijack attacks, not even to BGP hijack attacks.

A similar tale can be told about the MANRS (Mutually Agreed Norms for Routing Security). It is another initiative that calls for ISPs and Internet exchange points (IXPs) to declare that they follow a certain set of actions to improve routing security. This includes announcement filtering (e.g., by using RPKI), maintaining ROA information up to date, and even publishing contact information to promote communication and collaboration between network operators. The number of organizations that declare adherence to MANRS has also increased recently and steadily, but not sufficiently.[8]

Technological awareness has not yet led to lessons being learned universally. One lesson has escaped the networking community and decision makers, even after the demonstrations of 2010 and afterward. Furthermore, the complexity of BGP continues to make it difficult to detect hijacks. For a variety of spontaneous reasons, route selection is sometimes hard to predict and varies without malicious intent. The easiest way to determine how to exploit BGP and get traffic to go through some otherwise unintended AS node en route is for a state or a criminal organization to have an otherwise legitimate node along major routes – a Point of Presence (PoP) located in a routing facility at key network intersections points in the global Internet. By these bad actors' masking as a legitimate node in the network, it is very difficult for other network elements to identify a nefarious node.

China Network Explosion – Hiding in Plain Sight

The global expansion of large Chinese ISPs into the backbones of national networks across the world makes IP hijack operations easier to conduct, and also makes IP hijack detection more difficult due to the scale and omnipresence of these providers. The number of Chinese PoPs in major locations around the world, especially outside of established democracies, has been steadily increasing. Two Chinese telecommunications providers in particular, China Telecom (CT) and China Mobile International (CMI), have significantly expanded their networks in the past decade. Both are now significant players in the global non-Chinese Internet traffic transit market, with extraordinary access to – and ability to divert – routine network traffic of major and minor nations globally, especially in recent years.

To evaluate Chinese providers presence in the global transit market, the Internet transit market was mapped over the last decade for important countries in Africa (South Africa, Nigeria, Uganda) and South America (Brazil, Argentina, Chile). In addition, a few small nations in Europe and Asia (Singapore, Israel, Finland) were also considered. Until 2018, these countries did not have a significant portion of their traffic routed via a Chinese transit provider. In June 2019, however, Brazil started seeing a sudden and, for this industry, quite large increase in Brazilian traffic carried by CMI out to the rest of the world, jumping from 0.5% to about 6% (see Figure 2). The majority of this increase came from Oi S.A. (previously known as Telemar, a large Brazilian telecommunications company), which started using CMI as the major upstream provider. As a major rising nation with considerable natural resources and population, the communications of political, government, commercial, and civic leaders of Brazil would be of considerable interest to the Chinese government.

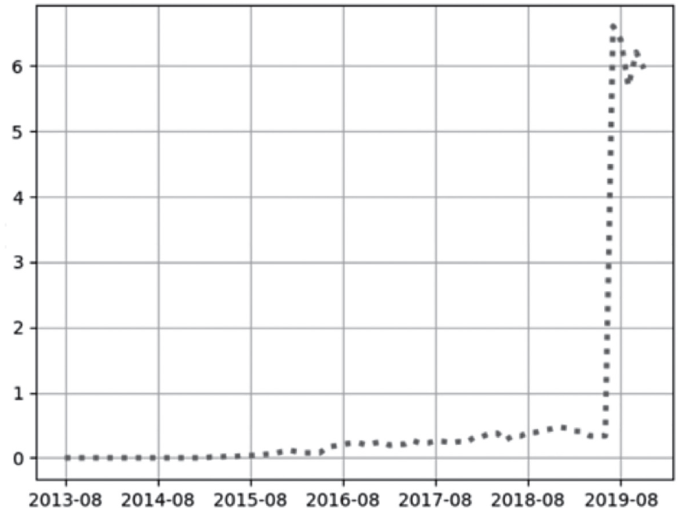


Figure 2: The Sudden 6-fold rise of China Mobile as a percentage of the Brazilian foreign transit market.

Across the sea but also in an area of considerable vast natural resources, Africa looms large in the global strategic influence and control agenda of China's state and commercial leaders.[9] In August 2019, several African nations increased the use of China Telecom as a provider, especially in Angola and South Africa (but also Nigeria, Namibia, and Kenya). At the same time, curiously, Russian TransTelecom – a peer of CT – started 'announcing' (via BGP) many African prefixes that it received from CT. As a result, a significant portion of the traffic of about 350 Address Prefixes (APs), mostly in Africa, started flowing through TransTelecom to and through China Telecom's PoP in Moscow even though intended for quite distant destinations. Nothing in the colloquial understanding of the Internet's design, which intended for data to travel by the shortest routes, would send traffic from South Africa to Israel through Moscow instead of through a major hub in western Europe, as shown in Figure 3. Once or twice, it could be a result of a mistake (a route leak) at TransTelecom or a change in the policy due to other political or economic reasons. However, TransTelecom and CT claim to be working together to shorten routes from China to West Europe.[10] It is not clear why TransTelecom would announce China Telecom routes to many peers in Europe in any case. That arrangement opens considerable opportunities for nefarious hijacking campaigns already well-demonstrated by China Telecom and its peer partner in Russia, TransTelecom.

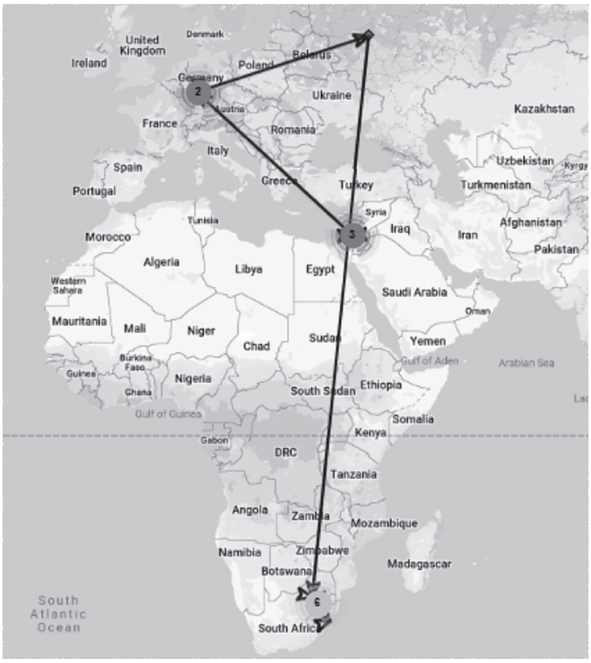


Figure 3: An example of a deflection through Moscow by TransTelecom and China Telecom. Routes between Israel and South Africa normally route through Internet exchange points in London or Frankfurt, where traffic is handed to African local or regional carriers that uses a submarine cable to transport traffic to Africa.

In the complex world of networks underpinning societies, bad faith players with a myriad of legitimate business footholds around the world are increasingly difficult to monitor, expose, and ultimately to get the political will to expel from the global transit market. Figure 4 demonstrates extraordinary increases in the transit traffic handled by CT in just one AP at the Africa nation – Zambia. Overnight, the portion of traffic towards this AP that is carried by CT grew from 0 to about 60% and a day later to about 85%. Namely, almost all the traffic to this and other APs in Zambia traversed the CT network. It is perhaps not coincidental that Zambia is also one of the nations whose government is being provided facial recognition technology by a Chinese vendor as well.[11] This increased Chinese penetration in the global transit market will challenge – and is likely to dampen the ability of – services that attempt to alert others against IP hijack attacks in real-time. Until recently, Chinese providers were not significant players in the global transit market, and it was relatively easy to identify hijacked routes based on (and we are oversimplifying here) the bare presence of a Chinese provider close to a local Western provider. With the integration of Chinese providers in the global transit market, considerably more and deeper analysis is needed to distinguish between legitimate routing through Chinese providers and malicious hijack attacks. Only recently have initial steps to use deep learning for this challenging task been published and the use of artificial intelligence (AI) for detecting such bad faith behavior is still nascent.[12] The response has been at best muted in the capitals of even Western democracies.

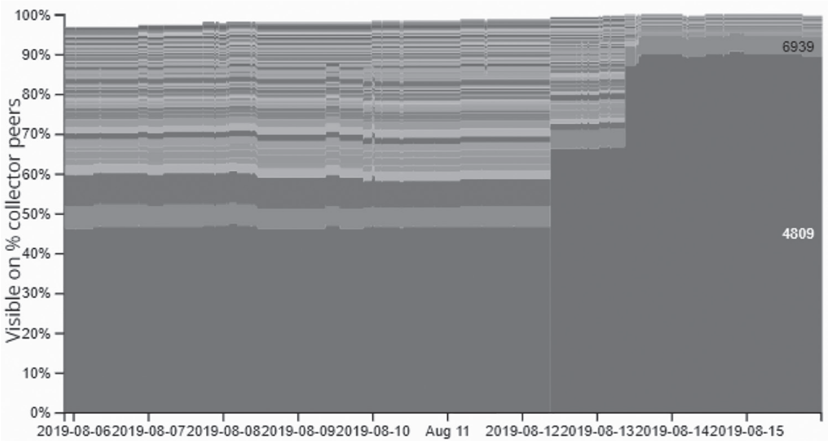


Figure 4: An example of the increase of traffic served by China Telecom (AS 4089) for an IP address block in Zambia during August 2019. CT share grew suddenly from zero to 60-85% for the rest of the month of August. This situation continued for several months.
The graph was generated using the RIPEstat site (stat.ripe.net).

Political Awareness Spotty – Action Resisted

If the technologists did not act to forestall an IP hijack despite evidence of the rise of Chinese telecommunications providers globally, political leaders of most nations were, and have been, even slower to react. Political and administrative communities in most established democracies rarely have any technical training or in-depth understanding of cyber threats to their networked infrastructures. When technical advisors are unable or unwilling to perceive the threats in the insecurity of the BGP global system, those they advise in political administrations will be commensurately even less responsive.

For the first six years of the 2010's decade, hijacking attacks were not dealt with publicly by Western democracies. Only in 2017, with the new US administration's generalized hostility to China, did attention to the cyber threat of network hijacks begin to have a toehold in the political debate about national security and the rise of a hostile peer power. By late 2018, in North America, our work on China Telecom BGP hijacking joined other reports about the undesirable behaviors of Chinese state champions, and the conversation about BGP hijacking moved from politically invisible to being perceived as a component of the general rise in cyber conflict – labeled here as "Great Systems Conflict" – with China.[13]

By early 2020, the Trump administration's actions against Chinese information technology corporations (many via Executive Orders) had finally spread to China Telecom – the central actor in the BGP hijacking noted in our late 2018 article.[14] A 2020 report[15] by the Senate Committee on Homeland Security and Governmental Affairs cited our previous work. In late 2020, the U.S. Federal Communications Commission (FCC) announced that it had begun a process of restricting China Telecom from operations in the US.[16] Six months later, in June of 2021, and under a new administration, the FCC announced it was imposing additional restrictions on US companies buying and installing telecommunications equipment from China.[17]

In Canada, in late 2018, the Prime Minister's national security adviser said that Canada would raise the traffic hijacking issue with senior Chinese officials at a security and legal affairs meeting in Beijing at the end of that year.[18] In February 2019, the Canada Parliament Standing Committee on Public Safety and National Security held a meeting that discussed the security risk from Chinese ISPs operating in Canada and the usage of Chinese-made telecommunication equipment in Canada's critical infrastructure.[19] Prof. Shavitt, one of the coauthors, was one of the two experts that testified in that meeting. Although Canada is acting to restrict Chinese firms in its telecommunications sector, it is resolutely moving much more discretely.[20]

Outside of North America, the political actors' awareness in established democracies of the ease and increasing threat from state-sponsored BGP hijacks has led to limited actions largely focused on one adversary – China. While all the 'Five Eyes' (i.e., Australia, New Zealand, UK, US, and more recently Canada) have taken steps to reduce their dependence on Chinese companies and telecom equipment, only recently has the biggest other actor (or bloc of established democracies) – the European Union (EU) – been willing to identify the potential for telecommunications misbehavior on the part of the Chinese specifically, let alone Russia, Iran, and others.

At the end of 2020, the EU and China signed an EU-wide bilateral investment deal – which every EU country has on its own with China save Ireland – in which China promised to allow EU companies into its home telecommunications market and ban forced technology transfers.[21] EU negotiating leaders signed the deal after over seven years of negotiations despite the known tendency of the Chinese government to make promises it does not keep on the ground, such as its original WTO admission agreement, and despite the clear evidence of a late-day quiet insertion by China of language enabling it to punish EU countries that decide to ban Chinese telecommunications companies Huawei or ZTE from their networks.[22] The efforts to ratify this trade agreement have currently been suspended. Other EU telecommunications-related restrictions, guidelines, and scrutiny on foreign vendors – especially on Chinese firms – have focused specifically on 5G equipment,[23] subsidies,[24] foreign direct investments screening[25] and takeovers or mergers,[26] and on guarding against economic competition and dependency from Chinese suppliers in strategic areas.

Missing from these actions is the nefarious use of otherwise normal traffic routes across all EU networks. Beyond that, there is little evidence of awareness of BGP hijacking attacks, no action, and no specific attention to Chinese telecommunications companies in this form of network attacks, even though it is known to the technologists across the EU. The problem cannot be solved by a nation here and a nation there if the wider global net is increasingly populated with PoPs and equipment owned and operated by states willing to act in bad faith.

CONCLUSION

This problem is not going to resolve itself in any way favorable to democracies unless their leaders and technologists acknowledge the evidence already abundantly present of an existential threat to the integrity of the Internet itself. It does not matter how strongly encrypted a data stream being shared across nations is if an adversary state or its proxies can routinely capture a copy of it and decrypt it at their leisure. As we noted in our 2018 piece, if legitimate and acceptable behavior cannot be assured, the footholds of the bad faith actor need to be expelled. Ironically, the Chinese government does not allow any foreign PoPs within China, indicating at least one nation where the lesson of BGP hijacking has been learned precisely because that nation knows what can be perpetrated. We suggested then, and repropose now, a policy of "Access Reciprocity" in which PoP presence by Chinese companies is matched, node for node and free presence for free presence, with overwatch and expulsion rules. The intent is to induce sufficient dedicated political and technical attention at the highest and lowest levels for a better balance between democratic and authoritarian information technology systems.[27]

Just before the final version of this article was ready to print, the FCC announced it will revoke China Telecom America's license to operate in the US.[28] This is certainly the outcome we were suggesting in this and our previous publication in 2018. However, that loss of license only affects CT's operations inside the US, not the wider operations or traffic hijacking by CT Global across any routes not transiting the US. Nor does it stop CT from using other services to carry its hijacked traffic as their own across the US en route to China or back to the original legitimate destination.

The great unlearned lesson of BGP hijacking is precisely that basic reciprocal fairness cannot be assumed unless it is ensured by fair and transparent processes that the bad faith actor cannot subvert. In an asocial global environment, having such a policy could be, as Robert Axelrod once noted, clarifying and effective in forcing hostile states to the table to cooperate on at least this one major threat.[29] Such an outcome is immensely desirable, but the window of opportunity to achieve it is quickly closing with the broadening and deepening presence of authoritarian state networks throughout the globe. It is time to learn this essential lesson and move to action. The US has made the first step in acting against this bad behavior by a state champion of China. We hope that Canada and other allies will follow suit.

NOTES

1. https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/.
2. Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs Journal* 3, no. 1 (October 21 2018), https://scholarcommons.usf.edu/mca/vol3/iss1/7/.
3. P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos, 2018, A Survey among Network Operators on BGP Prefix Hijacking". ACM SIGCOMM Computer Communication Review (CCR) 48(1):64–69, Jan 2018.
4. Geoff Huston and Randy Bush. 2011. "Securing BGP and SIDR". IETFJournal7, 1 (2011).
5. Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, H. Shulman, "Are We There Yet? On RPKI's Deployment and Security, NDSS, 2017.
6. https://rpki-monitor.antd.nist.gov/.
7. Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. "o Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today", Passive and Active Measurement (PAM) 2020, pp 71-87
8. Cristian Hesselman et al., "A responsible internet to increase trust in the digital world," *Journal of Network and Systems Management* 28, no. 4 (2020).
9. Celine Sui, "China-Africa Economic Relationship," *Courting Africa: Asian Powers and the New Scramble for the Continent* (2020).
10. https://company.ttk.ru/page4219071.html#!/tproduct/142079272-1520861032521.
11. Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents - Employees embedded with cybersecurity forces in Uganda and Zambia intercepted encrypted communications and used cell data to track opponents, according to a *Wall Street Journal* investigation," *Wall Street Journal,* August 15 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
12. Tal Shapira and Yuval Shavitt. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding. ACM SIGCOMM 2020 Workshop on Network Meets AI & ML (NetAI 2020), August 2020.
13. https://cyberdefensereview.army.mil/Portals/6/Documents/2021_spring_cdr/COVID_CDR_V6N2_Spring_2021_r4.pdf.
14. https://www.washingtonpost.com/national-security/trump-administration-moves-against-chinese-telecom-firms-citing-national-security/2020/04/10/33532492-7b24-11ea-9bee-c5bf9d2e3288_story.html.
15. https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
16. https://www.reuters.com/article/usa-china-tech/fcc-begins-process-of-halting-china-telecom-u-s-operations-idUSKBN28K2ER.
17. https://www.nytimes.com/2021/06/17/technology/fcc-china-technology-restrictions.html.
18. https://www.theglobeandmail.com/politics/article-china-telecom-hijacked-internet-traffic-in-us-and-canada-report/.
19. https://www.ourcommons.ca/DocumentViewer/en/42-1/secu/meeting-149/evidence.
20. David Ljunggren, "Canada has effectively moved to block China's Huawei from 5G, but can't say so," *Reuters*, August 25 2020, https://www.reuters.com/article/us-canada-huawei-analysis/canada-has-effectively-moved-to-block-chinas-huawei-from-5g-but-cant-say-so-idUSKBN25L26S.
21. https://thediplomat.com/2021/01/the-pitfalls-of-the-china-eu-comprehensive-agreement-on-investment/.
22. https://www.scmp.com/economy/china-economy/article/3116896/china-tried-punish-european-states-huawei-bans-adding.
23. https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/.
24. https://www.bloomberg.com/news/articles/2021-04-27/eu-threatens-fines-and-merger-bans-for-chinese-state-firms.
25. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200924_Chinese_Tech.pdf.
26. https://fortune.com/2021/05/05/eu-china-europe-restrictions-foreign-takeovers-investments-margrethe-vestager/
27. Demchak and Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking."

NOTES

28. Simon Sharwood, "China Telecom booted out of USA as Feds worry it could disrupt or spy on local networks - FCC urges more action against Huawei and DJI, too," The Register, October 27 2021, https://www.theregister.com/2021/10/27/china_telecom_booted_out_of/.
29. Robert Axelrod and William Donald Hamilton, "The evolution of cooperation," *science* 211, no. 4489 (1981).

The Need for National Cyber Insurance – A Lesson to be Relearned

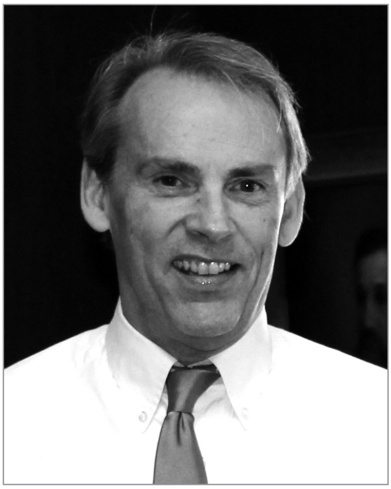
John T. Harvey

Securing a nation's cyber borders requires a high degree of coordination and openness among the relevant units, including real-time information sharing and threat assessment. Unfortunately, however, not only is there little incentive for private sector entities to voluntarily offer the necessary level of cooperation, but policy makers in free societies are reluctant to force such measures on them. Even more unfortunate is the fact that the threats are real, substantial, and have the capacity to have an adverse impact far beyond the initial point of incursion. This raises the question as to whether or not there exist yet-to-be learned lessons that could point us toward a means of motivating businesses and other institutions to accept what would otherwise be unwelcome intrusion and expense.

Defending in Cyberspace

This paper answers with a resounding yes and explains why the nation's cyber defense would greatly benefit from a study of the highly successful historical precedent set by the Federal Deposit Insurance Corporation (FDIC). The problem in that era was that the incentives created by the profit motive were not conducive to systemic stability. Particularly during expansions, individual banks tended to follow portfolio management practices that made them increasingly vulnerable to shocks. Greater risk carries the potential for greater return, and during an upturn, economic agents are inclined downplay risk (Minsky 1986). Competitive pressures may lead others to follow suit, and when and if trouble does emerge, those at the center can be expected to hide the details for as long as possible. Even if this behavior is confined to a minority of institutions, the fact that the financial system is an interconnected web of obligations means that a ripple in one sector has the potential to become a tsunami elsewhere. The situation in cyber security is very similar. Lax security practices—like risky assets—promise greater short-run returns; and, so long as they

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.



John T. Harvey is Professor and Chair of the Department of Economics at Texas Christian University, where he has been employed since 1987. His areas of specialty include international economics, macroeconomics, and contemporary schools of thought. He has served as Executive Director of the International Confederation of Associations for Pluralism in Economics, a member of the board of directors of the Association for Evolutionary Economics, a member of the editorial boards of the American Economist, American Review of Political Economy, the Critique of Political Economy, the Encyclopedia of Political Economy, the Forum for Social Economics, the Journal of Economics Issues, and the Social Science Journal, and was the lead editor of World Economic Review. John has won several teaching and research awards at his institution.

While he has two publications in Military Cyber Affairs, John is first and foremost an economist. His interest in cyber conflict is a function of his long-time fascination with international relations, conventional warfare, and wargaming.

are successful, competition may force others into similar cost-cutting measures. If a successful attack does occur, it is in the best interest of the victim to cover this up—even if there is the potential that it is affecting others as well and the consequences may become much more serious. In both cases, the individual incentives created by the profit motive can contribute to systemic instability. And again, in both cases, it behooves us to develop policies that tie system stability to individual profitability.

The FDIC and Financial Stability

As suggested above, the financial sector is inherently unstable. This is a problem because we need banks and other financial institutions to be on a sound financial footing so that they can provide the credit needed to fund consumer and business spending. A financial market failure can be crippling. Unfortunately, risk and return are inversely correlated and during an economic upturn, banks, etc., show a strong tendency to steer away from safer assets to more profitable but riskier options. This means that throughout the expansion, they are creating increasingly fragile portfolios. Hence, when the next downturn arrives, it is all the more severe, and recovery will be all the more difficult.[1]

This boom-bust cycle is precisely what was witnessed during the 1920s and 1930s. The 1920s demonstrated high rates of growth and low unemployment, the latter as low as 1.9% in 1926 and 3.2% in 1929, just before the recession hit. As expected, banks took on more risk (Calomiris and Wilson 2004: 422). So long as the expansion continued, there appeared to be no need for caution, and there was lots of money to be made. As we know, however, the expansion did not continue, with the economy peaking in late summer of 1929. Throughout the entire decade of 1920s, there had been roughly 6000 bank failures, generally among smaller, rural institutions, already considered to be less stable (FDIC 1984: 33). By contrast, in just the first four years of the

[1] See https://scholarcommons.usf.edu/mca/vol3/iss1/4/ for an explanation of the business cycle.

Depression, not only were there over 9000, but these were spread over what had been considered much more secure enterprises (Martens and Martens 2021). There is little question that this historic collapse contributed substantially to the severity of the Depression, and that banks' fragile portfolios were a significant contributor (Benmelech, Frydman, and Papanikolaou 2019).

Because those failures had consequences well beyond the solvency of the individual institutions in question, the government became involved. Though not without controversy, the Banking Act of 1933 was eventually passed, and it included the creation of the FDIC (FDIC 1984: 40). The final version (based on the Banking Act of 1935) included, first, an admission audit for new banks. Those banks then had to agree to additional monitoring above and beyond existing state and federal requirements. The FDIC assessed "the adequacy of the bank's capital, its future earnings prospects, the quality of its management and its usefulness in serving the convenience and needs of the community." (FDIC 1984: 52). And, of course, there was a subscription to be paid.

Bank failures fell from over 4000 in 1933 to just 370 from 1934 through 1941.[2] This was not solely due to the introduction of the FDIC, but the presence of the FDIC was a major factor. And, despite a subscription fee and the requirement of an admission audit and monitoring thereafter, banks—though initially reluctant—eagerly joined once they saw how successful the program had proved (FDIC 1984: 50). Indeed, FDIC insurance became a competitive advantage, with telltale advertising stickers on the door that advertised to the public that their deposits would be safe. Meanwhile, the event against which banks were insuring themselves became far less frequent—which of course was the real goal of the program. The financial system was the intended beneficiary, not the individual banks.

It has not always been clear sailing since then, of course. The deep recession of the early 1980s saw bank failures rise to a peak of 119 (1982), during the Savings and Loan Crisis (1986 through 1995) they averaged over 200 per year, and after the Financial Crisis over 400 banks failed (2008 through 2011). In addition, adjustments have been made to the original regulations. But it is difficult to argue that it has not been a success. Indeed, just a year into the program, the banking industry dropped its "fierce opposition" "in the face of the success of deposit insurance" (FDIC 1984: 50).

Elements of a Federal Cyber Insurance Corporation (FCIC)

A similar achievement is possible in the context of US cybersecurity. The situation is analogous: there exists a critical vulnerability in a key element of our national infrastructure, one that can be mitigated if agents followed more prudent policies and permitted a third party to monitor their activities (possibly in real time). It cannot be ignored because the consequences could be dire, and they go well beyond those directly involved. Unfortunately, individually they have still little incentive to cooperate to grow the program to the scale necessary to make it

[2] Data from FDIC: https://banks.data.fdic.gov/explore/failures.

nationally effective. For each agent or enterprise, participation would include surrendering more autonomy and privacy than would be necessary if they simply signed up with a private insurer. If we are reluctant to use a stick however, then we can use a carrot: insurance.

The principles underlying an FCIC would include:

- An overriding goal of securing US cyber borders, achieved by inducing private entities to follow expert-specified protocols and allow real-time information monitoring and sharing and crisis response. *Other features (e.g., the insurance program itself) are merely a means to this end.*
- Within that context, while it will be necessary to devise a schedule of pay outs for various event categories, *the FCIC is not an attempt to solve the puzzle of creating an economically efficient means to price cyber risk*. Again, federally sponsored insurance is but a means to an end. Indeed, private-sector options already exist, however their ability to address systemic problems is limited. They have no incentive to forward information to a central authority capable of determining the possibility of wider attacks, no incentive to reach out to possible targets who are not already customers, and limited financial ability to payout losses (not to mention the difficulty in pricing that they face).
- Given the degree of intrusion by federal authorities that would be required, insurance coverage pricing would have to be quite low to induce robust participation. However, it is important to remember that banks, at first reluctant, embraced the FDIC once it became successful.
- Since the program, unlike the FDIC, would not be self-financing, a working FCIC must be funded entirely by the federal, not state or local governments, because the federal government alone is free of a budget constraint.
- As with the FDIC, the expectation is that even if there is a monetary cost to the program, it would be a net gain for the US with a discernable decline in frequency and severity of costly events.
- Private-sector cyber insurance could be negatively impacted, but this is often true when the national interests are paramount, as here, where added security has become essential.

The outline below further reflects on these essential elements.

Securing the US Cyberspace as Overarching Goal

Cybercrime, cyber espionage, and cyber warfare are serious issues. The frequency and severity of attacks continue to increase, with one projected cost to the world's economy pegged at $10.5 trillion by 2025 (Morgan 2020). And while there is a tendency to monetize and aggregate costs into a single number, the reality is far more complex. How does one really put a price on the lost schematics of a weapon system or the infiltration of a power grid? Nor does anyone need to be convinced that the US is vulnerable.

Eliminating all threats is not feasible, but there are means of limiting them. While non-democratic nations can limit freedoms and resources in order to combat threats, the U.S. must entice private sector cooperation. This is where federally sponsored insurance can play a role. A basic element of an effective program would be well-defined best practices that all insured must follow to qualify. The FCIC would depend critically on this work. Most authorities agree that the overwhelming majority of breaches result from human error, with some projecting this cause as high as 95%, and techniques themselves may be far less important than continuous training and monitoring (The Coyle Group 2019). But federal agencies could easily provide, indeed require, the training (and do now in some cases), and monitoring should be added to their duties, as a vital component of any successful defense.

Pricing is no doubt the greatest challenge, and the primary reason we do not already have a vibrant private sector market for cyber insurance. It has thus far proven impossible to create actuarially reliable estimates of the cost and likelihood of the relevant events (Kshetri 2018). This is not to say that there has not been some promising growth, but in any event the FCIC's goal would not be to develop an ideal means of evaluating risk, but to induce firms to adopt policies that enhance system-wide resilience. Fortunately, one key advantage of public sector insurance is that there is no need to earn a profit. This means that creating reliable forecasts of the likelihood of specific events, with margins of error small enough to ensure the financial viability of the insurance provider, is not an issue. If there is a cyber event, the cost is evaluated–something we already do–and payment is made. It would be necessary to establish how the latter is calculated, but *a priori* risk assessment–normally an expensive component of insurance–is unnecessary. Ironically, public sector insurance could potentially contribute to the data set necessary to determine various probabilities and thus help create an industry for those who would like to offer supplemental or alternative insurance.

If these calculations are not being made, then one might fairly wonder how financing would be determined. For the FDIC, it is via subscriptions. The same could be done with the FCIC, but it is important to recall that while FDIC was initially very unpopular with the banking industry, it became law due largely to its immense popularity with the general public. Cyber insurance is unlikely to command mass appeal, so its passage may depend much more heavily on making it financially attractive to those desiring insurance. Funding via subscriptions would create an obstacle to this goal. If a subscription is to be charged, it could be a token amount based on the firm's annual revenues or profits. Or it could be entirely free: firms are covered by the cyber insurance if they adopt the practices outlined by the FCIC and they permit random audits and real-time monitoring. I suspect that this would be necessary.

Assuming no subscription fee, then data from 2016 suggest that payouts would add around 3% to the federal government's budget (based on the high-end estimate of the cost of cybercrime that year of $109 billion and a federal budget of $3.9 trillion; Chalfant 2018). This is with no reduction in the frequency and severity of the breaches, disruptions, etc., which is of course the primary goal of the program.[3] Where do we get the extra money? The same place we found

[3] This also does not count any administrative costs, which would be somewhat mitigated by the fact that existing agencies could either take on the tasks or supply the data necessary to pursue them.

the $2 trillion for the CARES Act in 2020 and the funding for World War II: we simply create it. In neither instance did we borrow dollars from another country or from our own people (who, in both instances, were still reeling from an economic shock: unemployment averaged 8.1% in 2020 and 9.9% in 1941). Resources are scarce, but money is not and it is impossible for the US to default in debt denominated in dollars (Kelton 2020). This has been more openly acknowledged by recent Federal Reserve chairs and is referenced here in a Federal Reserve Bank of Kansas City publication: "As the sole manufacturer of dollars, whose debt is denominated in dollars, the US government can never become insolvent, i.e., unable to pay its bills" (Fawley and Juvenal 2011: 5). Inflation is a potential problem if we continue to stimulate the economy via deficit spending when it is already at full employment, as we did in World War II (when unemployment fell to 1.2% and wage and price controls became necessary). Otherwise, there is no reason to expect inflation to be any more of an issue than it was after the Financial Crisis when in the ten years following the $840 billion American Recovery and Reinvestment Act of 2009, average annual price increases were 1.76%–the lowest of any decade since World War Two.

Another reason why the federal government should help absorb the cost makes sense is that "the US government is likely to end up footing the bill should a catastrophic cyber incident occur" (Knake 2016: 1). Because an ounce of prevention is worth a pound of cure, we should not wait for the disaster to occur but instead act today. As an analogy, consider the impact of Hurricane Katrina. In the end, the federal government financed $114 billion of the recovery (total damage was estimated to be $161 billion; KPRC 2018). Meanwhile, the cost of repairing the levees around New Orleans is estimated to be $200 million, or 0.18% of the amount contributed by Washington (Perlstein 2019). This is not to suggest that the levees alone would have prevented all the damage, but the difference in cost is staggering. And just because the federal government is not budget constrained does not mean that there is not a real savings here. Those dollars were used to activate resources, and many fewer would have been necessary to limit the damage done than were employed to clean up after it. The same is true in cyber.

An essential element of any successful FCIC would be conditioning pay outs on the insured fulfilling membership requirements. These could include the following (based on top cost mitigating factors identified in Ponemon 2020: 42):

1) Forming an FCIC-trained incident response team.
2) Adhering to FCIC-monitored incident response testing.
3) FCIC-approved artificial intelligence platforms and automated breach orchestration.
4) FCIC and Insured Red Team testing.
5) FCIC-supervised employee training.

Also critically important is real-time sharing of data and monitoring by FCIC and periodic audits, with payout discounts whenever, post-incident, there are findings that protocols were not followed.

One issue deserving consideration is the impact on private industry. It has been raised as a concern that a government program could end up crowding out the private sector (Knake 2016 and Woods and Simpson 2017). I do not think that there is any doubt that this would be the case. However, the same is true when we consider the impact of public police protection on private security firms, public libraries on bookstores, public schools on private schools, and so on. This is always the case when we determine that the volume of a good or service forthcoming because of the profit motive falls short of that we believe is in the public interest. Firms would still be free to purchase supplemental insurance and the data collected by the FCIC could be freely shared with private insurers so that they could more accurately price various risks. But in any event, the impact on private insurance should not be a reason not to pursue this avenue.

Lessons not Learned

This essay is not the first place where such a solution has been suggested. Knake (2016) and Woods and Simpson (2017) offer excellent analyses of the costs and benefits of public-sector insurance and describe other governmental efforts to induce industry to adopt safer standards. Despite this and the obvious example of the FDIC, however this lesson has not been learned. No one should expect it to be a panacea or a cure-all, but it would nevertheless put us in a much better position to defend our cyber borders. And, as the massive attacks of 2020-21 have demonstrated, time is now to act (Schneier 2020).

Our national infrastructure and our underlying cyberspace substrate is vulnerable to disruption and collapse and our intellectual property to sabotage and theft. If followed, fast- and ever-evolving best practices and guidelines exist that, will greatly reduce vulnerability, but they cost money. As in 1933, the cyber threat presents us with a range of choices today to include (a) private sector coverage that is partial or substantially complete, (b) public sector coverage that is wholly or partially subsidized, and (c) no coverage (i.e., self-insured.) Accompanying these alternatives again is a range of policies that would include mandated government audits and access to monitor compliance. As is true in the banking industry, some institutions are FDIC-insured, which requires compliance with certain mandated standards, and others are uninsured. If that could be accomplished, then offering insurance against losses from cyber-attack would have a similar effect on cyber resilience that the FDIC had on financial stability. And, just as with the FDIC, the insurance is secondary; the policy is about the system, not the individuals therein.

Thus far, applying this nationwide solution to national cyber security has received very little attention and, where it has, it has been unfairly discounted. This chapter will argue that this is a lesson not learned in the US in particular. We do not have the ability to eliminate cyber risk any more than we can banish bankruptcies, but we can absolutely learn from the FDIC how a Federal Cyber Insurance Corporation (FCIC) might reduce their frequency and severity.

NOTES

E. Benmelech, C. Frydman, and D. Papanikolaou, 2019, "Financial frictions and employment during the great depression," *Journal of Financial Economics*, 133(3), 541-563.

C.W. Calomiris and B. Wilson, 2004, "Bank capital and portfolio management: The 1930s "capital crunch" and the scramble to shed risk," The Journal of Business, 77(3), 421-455.

M. Chalfant, 2018, "Cyber crime costs global economy $600B annually, experts estimate," The Hill, Feb 21, 2018, accessed February 19, 2021, https://thehill.com/policy/cybersecurity/374854-cybercrime-costs-global-economy-600-billion-annually-experts-estimate.

The Coyle Group, 2019. "95% Of Data Breaches Are Caused By Human Error." The Coyle Group Risk Management Blog, December 30, 2019, accessed February 18, 2021, https://thecoylegroup.com/95-of-data-breaches-are-caused-by-human-error/

B.W. Fawley and L. Juvenal, 2011, "Why health care matters and the current debt does not," The Regional Economist, Federal Reserve Bank of St. Louis, 19(4), 4-5, accessed February 19, 2021, https://www.stlouisfed.org/publications/regional-economist/october-2011/why-health-care-matters-and-the-current-debt-does-not.

Federal Deposit Insurance Corporation (FDIC), 1984, Federal Deposit Insurance Corporation: The First Fifty Years: a History of the FDIC, 1933-1983, Washington, D.C.: Federal Deposit Insurance Corporation.

J.T. Harvey, 2018, "An Economics Primer for Cyber Security Analysts," Military Cyber Affairs, 3(1), article 4, 1-44, https://scholarcommons.usf.edu/mca/vol3/iss1/4/.

S. Kelton, 2020, The Deficit Myth: Modern Monetary Theory and the Birth of the People's Economy, New York: Public Affairs.

R.K. Knake, 2016, "Creating a Federally Sponsored Cyber Insurance Program," Council on Foreign Relations, Cyber Brief, November 2016, accessed February 19, 2021, https://cdn.cfr.org/sites/default/files/pdf/2016/11/CyberBrief_Knake_Cyber-Insurance_OR.pdf.

KPRC, 2018, "How much money has federal government paid to cover hurricane damage?" KPRC-TV, Houston, accessed February 19, 2021, https://www.click2houston.com/weather/2018/01/29/how-much-money-has-federal-government-paid-to-cover-hurricane-damage/.

N. Kshetri, 2018, "The Economics of Cyber-Insurance," IT Professional, 20(6), 9-14.

H.P. Minsky, 1986, Stabilizing an Unstable Economy, New Haven: Yale University Press.

P. Martens and R. Martens, 2021, "Wall Street's Casino Banks, Taking Deposits from Savers, in 1929 and Today," Wall Street On Parade, January 4, 2021, accessed February 11, 2021, https://wallstreetonparade.com/2021/01/wall-streets-casino-banks-taking-deposits-from-savers-in-1929-and-today/.

S. Morgan, 2020, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, November 13, 2020, accessed February 18, 2021, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

M. Perlstein, 2019, "New Orleans' levees won't be up to standard as early as 2023; Louisiana will need $200 million to fix them." WWL-TV, New Orleans, LA, accessed: February 19, 2021, https://www.wwltv.com/article/news/investigations/new-orleans-levees-wont-be-up-to-standard-as-early-as-2023-louisiana-will-need-200-million-to-fix-them/289-97215927-1d99-4383-a1b9-9f1e1494430e.

Ponemon Institute, 2020, "Cost of a Data Breach Study: Global Overview," Benchmark research sponsored by IBM Security independently conducted by Ponemon Institute LLC, accessed February 19, 2021, https://www.ibm.com/security/data-breach.

Bruce Schneier, 2020, "The US has suffered a massive cyberbreach. It's hard to overstate how bad it is," The Guardian, December 23, 2020, accessed February 19, 2021, https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols.

D. Woods and A. Simpson, 2017, "Policy measures and cyber insurance: A framework." *Journal of Cyber Policy,* 2 (2), 209-226.

Conclusion

Conclusion: When Experience Speaks and Too Few Listen – Curating the Unlearned Lessons

Chris C. Demchak[1]
Francesca Spidalieri

The past decade has ushered the rise of a ‘Cyber Westphalian,’ increasingly conflictual world characterized by rising great power competition, which now has escalated into ‘Great Systems Conflict’[2] across all digitally dependent societal domains. These struggles are occurring for, through, and enabled by cyberspace, and are now well in evidence globally. Yet, after ten years of experiments in creating organizations, strategies, policies, and offensive campaigns, consolidated democracies have either neglected or missed some valuable lessons. The essays in this special issue provide a broad overview of what was missed, ignored, mistaken, or simply not learned despite indications and experience. They also offer a way forward to tackle some of the more complex issues discussed. The unlearned lessons identified here range over issues of strategic approach, national scale and capacity, institutional change, and the socio-technical-economic system’s framing of the cybered conflict challenge. The authors here—subject matter experts with considerable and well-recognized expertise—are concerned about what we collectively are failing to appreciate and act upon. They intend by these essays to inform future national strategies, policies, and institutions to ensure that these unlearned lessons do not turn into future strategic failures in a rising, deeply cybered, post-westernized, authoritarian world.

This final essay offers a brief overview of these critical unlearned lessons.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

Strategy Unlearned Lessons

For starters, neglect of strategic lessons in a rapidly evolving and increasingly conflictual cybered world is particularly troubling. Today's larger powers find themselves in a growing struggle over global governance, pitting a democratic model that endorses the rule of law against an authoritarian alternative driven by centralized social control and arbitrary use of power. In this struggle over the digitized world order, cyber insecurity has emerged as both a sovereign issue and an international challenge prompting a multiplicity of discussions at the United Nations (UN) and in other international fora about internet governance and how to constrain harmful state behavior in cyberspace. Unfortunately, after almost twenty years of discussions and negotiations on the threats of malicious state activity in cyberspace and on the relevance of international law related to conflict in and through cyberspace, the diplomats and international lawyers of consolidated democracies have succeeded in negotiating only *non-binding* norms on responsible state behavior in cyberspace published in much publicized high-level UN reports.[3] In all these negotiations, they ignored events over the last two decades in which states freely used cyber tools for their political, economic, and military objectives, often in violation of the same norms they had underwritten and largely without any negative consequences. The paucity of concrete effects of these paper norms demonstrated a widely unlearned lesson about precisely what international binding law is, how it is actually created, and how it differentiates from voluntary norms, in particular, that norms only become legally binding when they are widely and consistently observed and enforced by states themselves. (Catherine Lotrionte, pp. 23-31) As a sad result, the two decades of discussions contributed more to the theatric appearance, but not the reality, of a cybered, safe, stable, and rule-bound global system.

Francesca Spidalieri is an Adjunct Professor for Cyber Policy at the University of Maryland's School of Public Policy and works as a cybersecurity consultant for Hathaway Global Strategies, LLC. She is also the Co-Principal Investigator for the Cyber Readiness Index 2.0 project at the Potomac Institute for Policy Studies, and the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University. In addition, Francesca serves as a cybersecurity subject-matter expert for the World Bank, the Global Forum on Cyber Expertise, the UN International Telecommunications Union, the EU CyberNet, and several other research institutes in Europe. Her academic research and publications have focused on cyber leadership development, cyber risk management, digital transformation, and national cyber preparedness and resilience. She lectures regularly at cyber-related events in the United States and Europe and contributes to journal articles and other publications on cybersecurity matters affecting countries and organizations worldwide.

Equally unlearned among the democratic like-minded communities is that states – and only states, not commercial firms, or civil groups – have the capacity, incentive, and legitimacy to negotiate with other states to find a common understanding and agreement on how to ensure a more stable, open, and interoperable cyberspace. Despite the demand from a wide range of civil society and private-sector actors for a role in international public policy for cyberspace, cybered conflict and diplomacy remain the purview of states. In this contest, states have a legitimate right and assumed obligation to defend their society and citizens. (Jim Lewis, pp. 33-39) Only when major powers agree to observe these norms, start to publicly attribute malicious cyber activity to other states, and invoke international law in their responses, these norms may actually develop into legally binding law over time.

There are other strategic-level lessons left unlearned on the table. Major lessons about the rising, biggest, and most formidable adversary yet – an increasingly authoritarian China – have taken a decade to be recognized, let alone acted upon. As the era of a dominant liberal international system declines with the rise of authoritarian-leaning states and Great Systems Conflict, the unlearned lesson was and remains that simply engaging with China will never deliver the hoped-for economic development and progressive normalization of society. Despite several decades of this Westernized politesse, China's government has not evolved towards an "autocracy-lite" regime that could play a more constructive and stabilizing role globally, as was expected by a wide variety of Western experts, economists, commercial leaders, and policymakers. The markedly illiberal turn that China has taken in the last decade came with demands for the international order to be modified to accommodate its emergence as a powerful strategic competitor and major global power. The seemingly surprised democracies continue to suffer not from a lack of knowledge but from a lack of cultural and historical context and a failure of imagination. Cloaked by a westernized “end of history” mindset blocking an accurate perception of reality, China has been free to turn Western dominance of information communication technologies (ICTs) into a significant vulnerability. In contrast, its regime has reinforced its domestic hold on power and shaped the international climate and some standard-setting bodies to favor its interests.

Even more "uncomfortable" lessons are yet to be learned. First, given the latitude accorded to China over the past two decades, Western power must now yield to pragmatism. Second, Chinese technology, like China itself, is here to stay and cannot be totally excluded from Western markets and, third, some of those technologies will inevitably be superior to those developed in consolidated democracies. Fourth, a US global leadership role is no longer assured as China will be a major economic player for the rest of the century. (Nigel Inkster, pp. 41-48) Unlearned strategic lessons about China have permanently changed the future for democratic like-minded nations who refused to see them.

Another pragmatic lesson is one that must be relearned from the Cold War – namely, that technology can offer some common ground between peer cyber competitors on which to build mutual trust and a common framework. Achieving cyber stability among cyber competitors is not predicated on congruence across all domains of cyber engagement but requires finding at least some areas of common interest or agreement and then engaging in confidence-building measures. This is a lesson learned during the Cold War, in which small science and technology teams from the US and the former USSR worked on joint projects provided these connections, enabling bilateral understandings despite hostility. This approach requires relearning that it can be more productive to narrow the problem-solving efforts to common and yet neutral problems to find plausible solutions that accommodate all positions and prevent potential escalation. (Chris Spirito, pp. 51-56) As the world increasingly reflects Chinese interests and priorities, learning this lesson can help open more pragmatic options to avoid constant escalation on the cybered conflict spectrum of the already emergent Great Systems Conflict.

National Capacity Unlearned Lessons

Moving from the strategic level to a more national or strategic-operational level, several lessons with implications for the pursuit of capabilities have yet to be learned. The first is that a functioning state must maintain its monopoly of force, which is critical for national viability in a conflictual cybered world. For most of the past decade, the bulk of the westernized democracies publicly disavowed offensive cyber capabilities save in their militaries to defend solely military forces. Yet, the lesson of a hostile cybered world is that a viable state cannot renounce its offensive cyber capabilities any more than it can refuse to defend the nation physically. Offense and defense in cyberspace are two sides of the same coin, and both are required, along with systemic cyber resilience, for robust cyber power.[4] For a state to have a competitive strategic advantage in cyberspace, become more resilient, and be able to effectively influence or convince others in international discussions or negotiations, it will have to learn to harness the right (and sufficient) talent, teams of experts, and competent senior leaders; fund national cyber resilience efforts with intent; and be willing to devote time and resources to "continuous, expensive, offense-informed, real-world trial-and-error experiments." (Sandro Gaycken, pp. 61-73)

Another strategic-operational lesson not fully learned by democratic states is the rising necessity for allies to work together in all aspects of national cyber security. The community of consolidated democracies will be an enduring minority of states, each facing a huge adversary like China and its fellow travelers such as a resurgent and aggressive Russia. Only with collective strategic and operational narratives and capacities can they defend their future and ensure the survival of democracy. For almost four generations, this lesson has been especially neglected in the US – the largest, wealthiest, and strongest among consolidated democracies. It has historically placed too little emphasis on the importance of such collaboratively developed strategic and operational narratives and decisions. In the Great Systems Conflict era, working with allies as peers is a critical, strategic-operational necessity. In a deeply cybered nation, whose entire socio-technical-economic system is struggling with massive onslaughts from state-sponsored attackers and criminals, defending alone leads to strategic and operational defeat over time (Ed Cardon, pp. 75-80). There are many other unlearned lessons about what contributions allies, team partners, private sector entities, and other organizations collectively operating in complex challenges can provide that would otherwise be unavailable, and these lessons need to be learned institutionally and strategically very soon. (TJ White, pp. 83-91)

Furthermore, a related unlearned lesson for the increasingly conflictual cybered world is that the expectations about some otherwise solid allies' help will have to be strongly nuanced according to their particular geopolitical and capability challenges. Some smaller states/partners cannot confront China in the way that only the US has the capacity to do. Their survival depends on a pragmatic balance between the two. Singapore is one such state – a small but highly connected island nation, considered a regional thought leader in cybersecurity. Despite having been both the target and the launching pad of significant cyber attacks (likely emanating from China), Singapore and similar neighboring ASEAN nations have often chosen not to publicly attribute such state-sponsored cyber incidents, carry out countermeasures, or showcase offensive capabilities. These choices were made to protect the safety of their intelligence sources, prevent escalation, or avoid harming their vital trade relations with China, as well as other pressing reasons. The risks of cyber conflict or adverse effects on trade for this highly connected nation are arguably too great for that tiny state to absorb, even if they are—in terms of values and longer-term preferences—clearly aligned with other westernized democracies. (Ben Ang, pp. 93-99) It is the example of such allies that can help the US to learn to be sensitive to the circumstances of its smaller and yet critical geo-strategically placed allies.

Another small but very capable partner with lessons to offer the US and its larger allies is Israel. Despite its small size, modest budgets, and limited natural resources, Israel has used a small nation's advantages in information sharing and coordinated policies to develop a comprehensive, whole-of-government, and whole-of-society national cyber security strategy and policies. It has succeeded in centralizing authority and resources required for national cyber defense, developing cybersecurity operational capabilities that allow for quick decisions and the ability to change directions when needed at relatively short notice, and fostering a thriving cybersecurity ecosystem and industry. The lessons behind this success have been available for some time but not learned by its largest ally. Indeed, the tendency among US policy makers has been to assume most of Israel’s lessons are not scalable to a nation the size of the US. Yet, many of the ignored lessons involve seeing Israel as a pilot project to develop more operational capabilities for whom scaling up is not the lesson. Rather, these lessons involve small-scale capabilities, irrespective of the size of the nation, such as assembling elite (non-military) groups of national cyber specialists ("cyber commandos") to tackle high-end techno-operational cyber-attacks. Another scale-indifferent lesson would be developing a more deterring or attacker-oriented response to cyber threats. Rather than narrowly using the U.S. Cyber Command (USCYBERCOM) or the National Security Agency (NSA) to react or focusing federal agency actions mainly on attribution (or naming and shaming, indictments, expulsions, demarche, designations, and sanctions), the US should learn the whole-of-society defense lesson of Israel. It should be developing nonmilitary “small elite teams” to answer the nationally relevant and exceptionally difficult techno-operational questions found in hunting state-level adversaries across society. Above all, the lesson from Israel is to provide this civilian commando team with top analysts and access to relevant data and tools, a "shielding bubble" protecting them from non-essential political and managerial interference, and to keep them small to maintain their agility. (Eviatar Matania and Lior Yoffe, pp. 101-109).

Policy and Organization Unlearned Lessons

Moving from the national or strategic operational level to the institutional level, for federal agencies or departments in the US, the lesson of importance and persistence was learned through cybered conflict, but only belatedly. It has taken a long time for a large power like the US to learn that perseverance in confronting an enemy’s cyberspace is necessary to effectively deter, constrain, thwart, and frustrate adversaries over time, preferably before they can achieve cumulative strategic effects. The concepts of “persistent engagement” and “defend forward” were first introduced in 2018 by USCYBERCOM and then incorporated by the U.S. Department of Defense (DoD) into their new cyber strategy. These approaches challenged the previously dominant assumptions and prescriptions of deterrence theory. Whether the state responds or not, the new presumption is that authoritarian states and non-state actors will always continue to conduct malicious cyber activities to protect their regimes, undermine political cohesion in the West, delegitimize democratic institutions, and reduce the economic, political, and military advantages of the US and its allies, etc. Before and after the publication of these documents, the evidence was clear that cyberspace campaigns against the US and its allies were continuous and ongoing, and that adversaries would persist given the low cost of entry, anonymity, non-timely attribution, ambiguous redlines, and the number of pervasive system vulnerabilities to exploit. Therefore, in 2018, the US began to learn the lesson that to compete and persevere, one requires persistence in engaging and seizing the initiative and in defending forward (outside system boundaries and as close as practicable to the source of malicious activity), not acting with restraint and episodic responses, and in anticipating rather than simply reacting or threatening future actions. (Emily Goldman, pp. 113-118) Ironically, this lesson resembles the constant engagement of naval forces during the Cold War, suggesting – not for the first time – the similarity of cyberspace to the ocean for a submarine and, thus, leading to the implication that this lesson is really just being relearned. However, many of our more advanced allies have yet to learn this lesson for even the first time.

If one is to engage persistently, then how is one to gauge effectiveness of the operations? Metrics – more precisely the lack thereof – constitute the soul of a further difficult to learn lesson, specifically for institutions trying to conduct defensive operations. Leaders need to comprehend the wider scale of the threats to balance all these responses. Resilience, competitiveness, and effectiveness rest on having an accurate vision of the scale and scope of cyber threats. Clear, objective, and repeatable metrics can help measure the success and effectiveness of cyber-related policies and initiatives in the deceptive and opaque cybered world. This lesson requires an emphasis on developing and employing metrics to measure the real impact of cybersecurity initiatives, such as whether efforts have effectively reduced the number of intrusions on critical systems or the impact of cyber-attacks. Such metrics are as yet unavailable. Agency, corporation, and state-level policies and operations are in effect shooting in the dark about whether procurement policies and acquisition rules appropriately incorporate cybersecurity standards and cyber resilience requirements; or where and how the private sector has adopted appropriate security measures and best practices that embody internationally recognized standards of care (e.g., encryption, MFA, patching, auditing, liability regime). Many questions are unanswerable without objective metrics. These include questions of how cyber issues impact citizens' security, privacy, and civil liberties; whether they have adopted cyber hygiene best practices; and whether international cooperation against cybercrime and cyber-enabled crimes has minimized the impact of serious attacks on society or reduced the number of safe havens for criminals. Without valid metrics, it is difficult to formulate informed and coherent policy or operations, let alone learn from the lessons of the past. (Harvey Rishkof, pp. 121-126).

Persistent engagement without metrics to gauge effectiveness can also lead to policy tunnel vision where some tools are repeatedly used, and others ignored. As one of the most connected ICT-dependent countries in the world, the US is at a distinct disadvantage if it limits responses to largely military-borne cyber operations and minimizes other diplomatic, information, military, and economic ("DIME") instruments of national power. The US needs to learn the lesson of adopting a smart and consistent use of all the DIME tools and resources already at its disposal to prevent and respond to future aggressions in, through, and enabled by cyberspace, while also strengthening partnerships and alliances across Western democracies and other global regions. (Michael Klipstein and Pablo Breuer, pp. 129-135)

Another lesson about not leaving options on the table in operations and policies concerns effectively integrating the inevitably significant role of private sector actors in a digitally conflictual era. They produced the underlying shoddy cyber substrate, and they now develop, operate, produce from, expand, maintain, and advance it technologically. Their operations are often on the front line of adversarial campaigns, and they are used as pawns in economic warfare. Their enterprises are targets of widespread theft of intellectual property to achieve later market control, or the victims of takeovers, investments, bribery, or blackmail. They are unable to force cyberspace to be more stable and secure when dealing with ruthless authoritarian states. However, the unlearned lesson is that they (and their interests) certainly have a role as advisors, implementors, and innovators to inform the international and collective allied operational negotiations conducted by states to assure national defense. (Andrea Little Limbago, pp. 137-149)

Socio-Technical-Economic Systems (STES) Unlearned Lessons

Having the private sector inside the defense tent does not mean better outcomes if they and the governments they support miss this another lesson about the integrated relationship between the underlying cyberspace and emerging new technologies and their increasing criticality across digitized societies: what infects the parent infects the child. Reaching across the strategic, national, and institutional levels, technological integration of a nation's socio-technical-economic systems (STES) strongly influences its basic load of cyber vulnerabilities that are passed on to the new emerging technologies. These new technologies are built on, meant to be embedded in, and will operate through the underlying cyberspace. The fundamental inability to secure that cyberspace is costing consolidated democracies 1-2% of their GDP annually[5] and is responsible for accelerating the rise of China as the chief adversary of the previously dominant liberal rule of law over the global system. The same security-averse tendencies that marked the computer vendors, internet promoters, and then paid cyber defenders of the original and shoddy cyberspace substrate are now leaving vulnerable the entire life cycle of emerging technologies, from artificial intelligence to quantum and so on. Unless and until that underlying cyberspace jumble is transformed into something securable, defensible, and resilient, emerging technologies built on it will remain vulnerable.

The apple does not fall far from the tree, and the tree must be transformed for the surrounding society to survive in the coming more authoritarian world. (Chris Demchak, pp. 153-160)

A particularly difficult and clearly unlearned lesson about national socio-technical-economic systems is how to prepare for the inevitability of failures in large complex digital systems. Given the level of integration across digitized societies, smaller failures can cascade into disasters, especially those that adversaries could start or help along. What might be called for is old-fashioned “prudence” in assuring ubiquitous alternatives and functional backups that can be used when – not if – complex catastrophic events occur. But backups must be regularly updated, tested, and maintained, not assumed to be available. Given the numerous problems of today’s cyberspace (including unethically designed embedded systems, unmanaged connectivity, and failure by design), the most important unlearned lesson boils down to the imperative that (analog) backup alternatives must not be let to wither. The only way to protect and thereby be systemically resilient as a nation is to have healthy and available analog equivalents providing the same services as the cybered functions on which so much relies. (Dan Geer, pp. 163-173)

Following on that systemic argument for an entire nation is another as-yet unlearned lesson: keeping less complex, opaque, and potentially unmanageable systems on hand to be able to function systemically when the adversary imposes surprise. This lesson is particularly critical for military forces like the U.S. Navy. Four questions underlie this lesson, and these must be answered before the service can be assured that it is resilient to the kinds of intrusions, disruptions, and even deception that the adversary China and any fellow travelers will attempt at scale, en masse, and repeatedly. The four questions on cybersecurity concern tradeoffs between security versus efficiency and convenience, the need for a less digitized reserve, the possibility of enforced autonomous systems use, and the obstacles to fleet design that achieves the Navy’s distributed maritime operations (DMO) concept. The Navy must answer these questions by examining its systems, procedures, doctrine, and force designs, lest the cyber vulnerabilities mean losing a conflict with a technological near-peer like China. (Sam Tangredi, pp.175-179)

A deeper unlearned lesson about democratic socio-technical-economic systems’ dependence on the cyberspace substrate requires recasting ‘content’ or data in cyberspace as infrastructure that needs protection and resilience as much as physical installations. Consolidated democracies must learn that data integrity, along with confidentiality and availability, must be given the same attention (and appropriate resources) as physical infrastructure. Content should not be conceptually separated from cyber security in discussions, policy, or defense operations. This lesson is particularly critical as the world heightens reliance on artificial intelligence (AI) and machine learning (ML) algorithms. These emerging technologies require large volumes of training data and are currently largely developed with little attention to cyber security during their lifecycle. (Sean Kanuck, pp. 181-190)

Furthermore, content rides among countries on international networks, and another lesson yet to be absorbed concerns the abuse of this complex connectivity by adversaries of democratic nations. Political and administrative communities in most established democracies rarely have any technical training or in-depth understanding of cyber threats to their networked infrastructures. They have not been aided by technical advisors who have been for two decades slow to perceive or unwilling to call attention to the threats buried in the insecurity of the same networks. Late in the last decade – in 2018 precisely, some senior leaders of national security communities of the US and other allied nations were informed about the increasing threat from state-sponsored hijacks by their major adversary – China – and other state-level bad actors. By then, many technologists across the network defense communities were willing to acknowledge awareness of these campaigns. Nonetheless, only a few consolidated democracies are attempting to counter these attacks with limited responses, likely too focused only on one actor – China – and only some of its corporate bad actors. These attacks have continued, indicating this lesson has yet to be learned. (Yuval Shavitt and Chris Demchak, pp. 193-205)

Finally, one surprising, unlearned lesson concerns the paucity of government support for cyber insurance. It is not an overstatement to attribute much of the stability in prosperity in the US to the rise of affordable and regulated insurance across sectors and products. Yet cyber insurance is currently burdensome to obtain, increasingly expensive, too narrow in coverage, and too focused on firms with large budgets. This is an unlearned lesson in the US even though there is already a successful model of a solution from broadly similar circumstances. The FDIC is a nearly century-old insurance scheme enacted to resolve similar and possibly catastrophic risks to the US banking system in the early 20th century. Like cyber incidents today, failures then (and now) in the banking system could (and did) quickly cascade to harm the entire national socio-technical-economic system and beyond. Like cyber today, medium and smaller firms had no chance of surviving without government help. A national cyber insurance scheme could provide multiple benefits across the national cyber substrate, including helping small and medium firms – the bulk of the internal economic activity and lifeblood of the national STES – learn better how to choose their technologies, operate them more safely, and be more resilient to the inevitable disruptions and failures. In short, governments defend their societies, and that should include creating public insurance for cyber just as they would nurture any other kind of societal resilience across sectors, locations, and threats. (John Harvey, pp. 207-214)

Concluding Remarks

By our account, there are at least 20 yet-to-be-learned lessons forming a converging picture of what has escaped our vigilance over the past ten or more years. From a systemic point of view, especially in using the framing of socio-technical-economic systems, the lessons form an overarching meta-lesson about systemic resilience and forward disruption as key components of national cyber power. The expert views discussed here clearly indicate that governments have a central role to play in building the nation's cyber resilience. Still, all sectors, whether private or public, need to be inside the cyber defense tent. These experts have pointed out several yet-to-be-learned lessons across cyber-related disciplines, from the need to use international law appropriately and negotiate at the state level intelligently with knowledge of the adversary and agilely on some topics but persistently standing firm on others with the necessary defense capabilities, service funding, and tailored teams, to absorbing the help and experience of allies big and small, and finally to rethinking the connectivity of and structure, technology, indemnification, and nondigitized reserves of the whole. The big picture painted by our experts suggests a fragmented narrative has blinded national political, economic, and technological leaders for a decade or more.

Unfortunately, the pock-marked and stubbornly dominant American zeitgeist that views national power from the triumphal twentieth-century lens of a remaining, untouchable, and immutable superpower, unfortunately, extended the same broken, unsystematic definitions to cyberspace. For over three decades of cyberspace's maturity, self-evident lessons have been obscured from the US and key democratic allies' views. By 2010, cyberspace was clearly identified by the US and several allies as a first-tier threat, yet the self-evident reality still struggled to be seen. Even top-tier master's degree schools feeding future leaders to senior agencies and corporations were largely oblivious in their curriculum to the rising threats of cybered aggressive state adversaries and crime.[6]

Now, over a decade later, after cyberspace was declared a top-tier threat by the US and several key allies, several key lessons remain unlearned. These lessons should have been obvious from the outset. Cyber power rests on the capabilities of a state to engage in legal forward disruption, but it also critically depends on the systemic resilience of that nation's socio-technical-economic system. And states smaller than China will eventually fall to its relentless pursuit to be the central global actor in international economic and technological interactions, unless these states gather to form a collective peer to jointly defend their collective technical and economic futures through a cyber operational resilience alliance (CORA). If they fight alone, China's rise, although bumpy here and there, is likely to reward the authoritarian state with the first seat among nations politically and inevitably socially, a slow form of vassalization of both democratic and non-democratic nations.

Allies in cooperation and joint operations, the central organizing role of democratic governments with private sector support, securable emerging technologies, analog backups and reserve forces, capable agile red teams focused forward, even public cyber insurance – all these unlearned lessons and more have been identified in this issue. And our experts explained the lessons' criticality to national power, especially in the various contributions to the cyber resilience of the nation. There are, of course, more unlearned lessons than those described here. However, if each of the democratic nations' public and private leaders act collectively on the lessons outlined here, the next issue on unlearned lessons might be much shorter. In that latter ideal case, a future special edition of *The Cyber Defense Review* would examine how consolidated democracies collectively succeeded at creating robust cyber power through national cyber resilience. Instead of schooling leaders on what they have not learned, the next set of authors could be offering a how-to manual on prosperity, security, and cooperation in a cybered world. Each of these essays implies that ten years is long enough for neglect and handing advantages to the rising peer adversary. One must act on these lessons before the options they offer today wither away. Current trends do not favor the democracies in the Great Systems Conflict era. Time has a way of running out for those who refuse to learn.

NOTES

1. All ideas in this essay are solely those of the authors and do not reflect the positions of any element of the US government.
2. Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *Cyber Defense Review* 6, no. 2 (Spring 2021).
3. For example, the consensus reports adopted by the UN Group of Governmental Experts (UN GGE) and the UN Open-Ended Working Group (OEWG) in 2021.
4. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, Georgia, USA: University of Georgia Press, 2011).
5. Melissa Hathaway, "Interview on Tiktok, Wechat, and U.S.-China Decoupling with Melissa Hathaway and Gary Rieschel," interview by Gary Rieschel, *Expert Discussion*, August 13, 2020, https://www.ncuscr.org/event/tik-tok-wechat-us-china-decoupling/video.
6. Francesca Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," *Pell Center for International Relations and Public Policies*, March 2013, https://salve.edu/sites/default/files/files-field/documents/pell_center_one_leader_time_13.pdf.

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

CyberDefenseReview.Army.mil

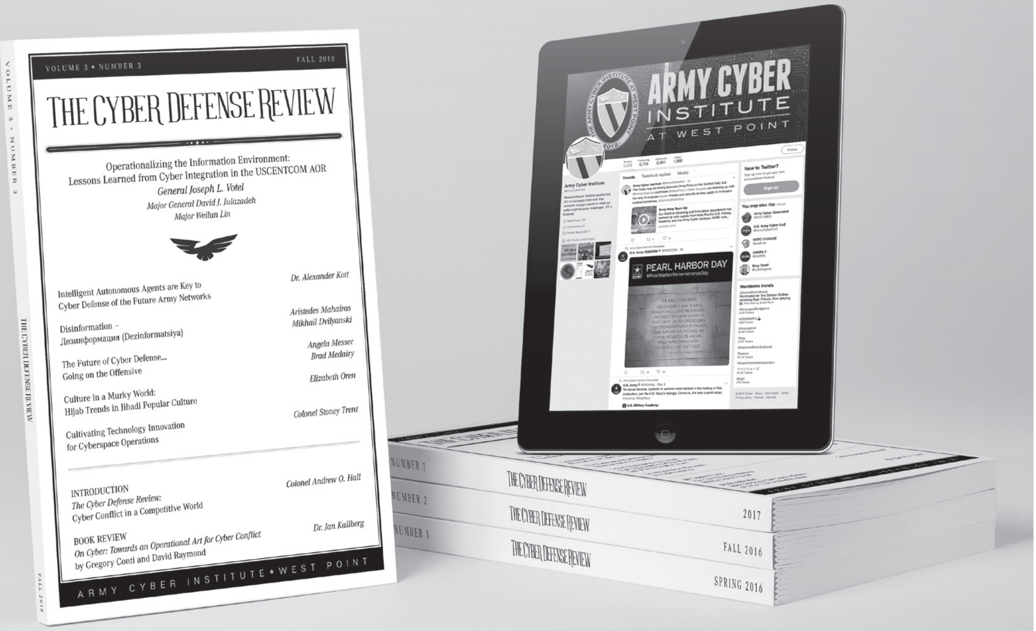
AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LInkedIn @LInkedInGroup

Twitter @ArmyCyberInst

@CyberDefReview


VOLUME 3 • NUMBER 3
FALL 2018
THE CYBER DEFENSE REVIEW
Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR
General Joseph L. Votel
Major General David J. Julazadeh
Major Weilun Lin
Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks
Dr. Alexander Kott
Disinformation – Дезинформация (Dezinformatsiya)
Aristedes Mahairas
Mikhail Dvilyanski
The Future of Cyber Defense... Going on the Offensive
Angela Messer
Brad Medairy
Culture in a Murky World: Hijab Trends in Jihadi Popular Culture
Elizabeth Oren
Cultivating Technology Innovation for Cyberspace Operations
Colonel Stoney Trent
INTRODUCTION
The Cyber Defense Review: Cyber Conflict in a Competitive World
Colonel Andrew O. Hall
BOOK REVIEW
On Cyber: Towards an Operational Art for Cyber Conflict by Gregory Conti and David Raymond
Dr. Jan Kallberg
ARMY CYBER INSTITUTE • WEST POINT
ARMY CYBER
INSTITUTE
AT WEST POINT
PEARL HARBOR DAY
NUMBER 1
NUMBER 2
NUMBER 1
2017
FALL 2016
SPRING 2016

ARMY CYBER INSTITUTE ◆ WEST POINT

THE ARMY CYBER INSTITUTE IS A NATIONAL RESOURCE FOR RESEARCH, ADVICE AND EDUCATION IN THE CYBER DOMAIN, ENGAGING ARMY, GOVERNMENT, ACADEMIC AND INDUSTRIAL CYBER COMMUNITIES TO BUILD INTELLECTUAL CAPITAL AND EXPAND THE KNOWLEDGE BASE FOR THE PURPOSE OF ENABLING EFFECTIVE ARMY CYBER DEFENSE AND CYBER OPERATIONS.