VOLUME 6 ◆ NUMBER 4 FALL 2021

THE CYBER DEFENSE REVIEW

Responding to Proxy Cyber Operations Under International Law

Lt. Col. Durward E. Johnson and Prof. Michael N. Schmitt

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

Fall 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.

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

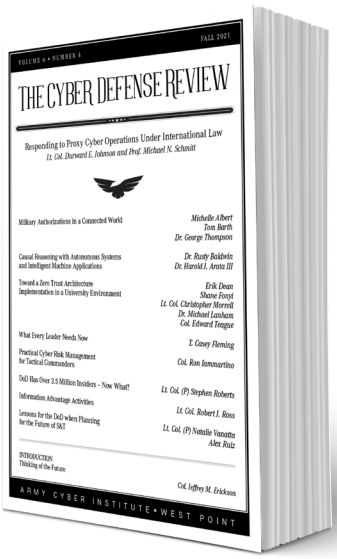
The Cyber Defense Review

Introduction

VOL. 6 ◆ NO. 4

The Cyber Defense Review: Thinking of the Future

Colonel Jeffrey M. Erickson



"It's tough to make predictions, especially about the future.""

–Yogi Berra (and many others...)

Since the publication of Johannes Kepler's novel, *Somnium*, science fiction has played an interesting role in society. It has been used to inspire (just ask how many current astronauts point to *Star Trek* as their reason for their chosen profession), to inform about possibilities (driverless cars have appeared in numerous films), or to serve as a warning (pick any post-apocalyptic movie...there's too many to list).

Many of the current cyberspace challenges we face were, at one time, the stuff of science fiction. While it is possible to fixate on the negative aspects of the current and future state, the many authors in this issue offer potential solutions for our challenges. Hopefully, their perspectives and proposals will move us beyond the status quo to reach a more advantageous state.

First, in the area of policy, our authors tackle the challenges of proxies and insider threats and propose solutions on where we need to go concerning these complex topics:

- **Cyber Proxies:** In "Responding to Proxy Cyber Operations under International Law," authors Michael Schmitt (Professor of International Law at the University of Reading in the United Kingdom) and U.S. Army Lieutenant Colonel Durward Johnson (Chief of Military Justice, III Corps and Fort Hood) discuss the challenges surrounding the use of proxies and the associated legalities and nuances concerning countermeasures. While there are current legal options, a more flexible interpretation and increasing

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.

use of these options will move DoD towards more effective deterrence.

- **Insider Threats:** Lieutenant Colonel Stephen Roberts (U.S. Army Cyber Command) poses an interesting question in "DoD Has Over 3.5 Million Insiders: Now What?" He identifies the risks (whether malicious or not) of having such a large number of individuals that may directly impact national security. He proposes a User Online Risk Score (UORS) model, similar to a FICO credit score, that measures a user's behaviors with respect to work to determine potential risks.

As technology continues to advance, DoD's approach to integration and implementation in future operations is critical, from the office to the battlefield.

- **Zero Trust Architecture (ZTA):** One of the evolving approaches to increase security in modern network environments is the Zero Trust Architecture. In "Toward a Zero Trust Architecture Implementation in a University Environment," the United States Military Academy (USMA) Information Technology team describes how West Point might implement zero trust principles to meet its mission as a premier academic institution while simultaneously serving as a U.S. Army organization.
- **Risk Management:** In his article, "Practical Cyber Risk Management for Tactical Commanders," Colonel Ron Iammartino (Army War College Fellow at Princeton University) proposes six decision rules that commanders can employ to take advantage of available technologies, services, and maintenance processes. Not only does this approach improve cybersecurity risk management, but it enables greater capability and adaption to cyber threats.
- **Artificial Intelligence:** The challenges with developing artificial intelligence through causal analysis are addressed in the article "Causal Reasoning with Autonomous Systems and Intelligent Machine

Applications," by Dr. Rusty Baldwin (University of Dayton) and Dr. Harold Arata (AT&T). By applying causal analysis to the fields of computer science and engineering, they argue that the potential for AI could reach the objective of human-like reasoning.

In addition to the technical aspects of the future environment, we are becoming more aware of the impact of complex information environment on individuals, societies, and nation-states.

- **Cyber Influence Operations:** In their article, "Military Authorizations in a Connected World: DoD's Role in Cyber Influence Operations," Michelle Albert, Tom Barth, and Dr. George Thompson (all from the Institute for Defense Analysis), discuss the challenges of competing in the gray zone and potential solutions to this capability gap. If we cannot find a way to win the "battle of the narrative" in the competition space, we may lose before the conflict even begins. This can be overcome with a new whole-of-government approach that includes relooking at existing laws and authorities. Sadly, while putting this issue together, we learned of the passing of Dr. Thompson. We are most grateful for his contributions to this issue.
- **Strategic Agility:** In "What Every Leader Needs Now: In This Unprecedented Era of Global Competition," Casey Fleming (Chairman and CEO of BlackOps Partners Corporation) calls for a cultural change in the business world with respect to the post-pandemic world. By applying the concepts of wargames used by military organizations, such as questioning assumptions, identifying/mitigating risk, and analysis of potential/likely future environments, businesses can set the conditions to evolve in the competitive space.
- **Information Advantage:** In "Information Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations," former ACI member and current Strategic Initiatives Chief to the Commanding General, Army Cyber Command (ARCYBER), LTC Robert Ross, proposes definitions and constructs to simplify the understanding of information and its relationship with future doctrine, information advantage, and the Army Warfighting Functions.
- **Forecasting the Long-Term Future:** In "Lessons for the DoD when Planning for the Future of S&T," ACI's Lieutenant Colonel Natalie Vanatta and advisor to the DoD, Alex Ruiz, describe the process they employed to inform the Office of the Under-Secretary of Defense (Research & Engineering)'s Science & Technology Roadmap which helps define potential technologies out to 2045. They touch on many of the complex factors affecting the current and future environments that must be addressed or mitigated to move DoD forward.

I hope these articles help stimulate your thoughts on the current state of the cyberspace domain and inspire you to look at setting conditions for a preferred future. I look forward to seeing you there (once we figure out *Star Trek*'s teleportation tech)!

The Cyber Defense Review

Senior Leader Perspective

Responding to Proxy Cyber Operations Under International Law

Lieutenant Colonel Durward E. Johnson
Professor Michael N. Schmitt

INTRODUCTION

The United States (US), its allies, and other partners are engaged in long-term strategic competition with Russia and China—near-peer adversaries adept at operating in the grey zone of international law, where the precise contours of the law are difficult to discern.[1] They do so to complicate our response options, in part to avoid provoking a direct military response.[2] Increasingly, cyberspace is that grey zone, a domain in which Russia, China, and other adversaries such as Iran and North Korea mount cyber operations ranging from cyber-enabled espionage, theft, and propaganda campaigns to significantly more disruptive and destructive operations. In particular, they often leverage non-state actors—cyber proxies—to do their bidding because proxies further complicate legal and policy assessments of the operations. And those assessments determine the response options available to victim states.

As a general matter, states agree that they "must not use proxies to commit internationally wrongful acts...[and] should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs [information and communications technology]."[3] The legal challenge is that the nature of proxy use differs from case to case, and these distinctions determine the lawfulness of responses. Russia's relationship with proxy groups provides a good example. At one end of the spectrum lies tacit approval of hostile cyber operations conducted independently by non-state patriotic hackers. Recall the large-scale denial of service (DDoS) cyber operations against Estonia in 2007 that shut down, among other things, government websites, key banks, and news outlets. Although the extent of its involvement remains murky, Russia's failure to condemn the operations and take measures to terminate those mounted from its territory evidence at least tacit approval.[4]

Lieutenant Colonel Durward E. Johnson is Chief of Military Justice, III Corps and Fort Hood, Texas. He was the Associate Director for Law of Land Warfare and Professor of International Law at the Stockton Center for International Law and the U.S. Naval War College in Newport, Rhode Island as well as the U.S. Army's senior operational law trainer at the Joint Multinational Readiness Center. He has also been a legal advisor deployed in support of military operations in Afghanistan and Iraq. LTC Johnson holds an LL.M. in Military Law from The Judge Advocate General's Legal Center & School, a J.D. from Loyola Law School, Los Angeles, and a Bachelor of Science from the University of Texas at Austin.

But the paucity of evidence as to Russian government involvement or control not only allowed Russia plausible deniability but also severely limited its adversaries' response options. At the other end of the spectrum, Russian security and intelligence services have directed hostile cyber operations by cyber proxies.[5] An example is the massive Yahoo data breach that began in 2014. Three years later, a U.S. federal grand jury indicted two Russian Federal Security Service officers for conspiring with cybercriminals to commit cybercrime and espionage.[6]

The relationships between proxy groups and governments usually fall between these extremes. Sometimes, states employ a multifaceted approach, as Russia did in its 2020 U.S. federal elections influence campaign, which included operations by "Russia's intelligence services, Ukraine-linked individuals with ties to Russian intelligence and their networks, and Russian state media, trolls, and online proxies."[7] Other recent incidents in which the precise extent and nature of Russian government involvement remains an open question include the Colonial Pipeline and JBS ransomware operations.

This article addresses an issue appearing in the Army's 2021–22 Key Strategic Issues List: "*Assess Russia's use of proxy or patriotic hackers and evaluate international laws and norms that can be used to limit their use*."[8] As will be illustrated, it is generally the interplay between the type of harm caused by a hostile cyber operation, the legal attributability of the operation to a state, and the legal nature of the proposed response that determines how the victim state may respond. Analysis begins with a discussion of the international rules most likely to be violated by either a proxy's hostile cyber operation or the proposed cyber response by the victim state. Those response options will also be determined by whether the proxy's operation can be attributed to a state as a matter of law, the subsequent topic addressed

Michael N. Schmitt is Professor of International Law at the University of Reading in the United Kingdom, G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point, Charles H. Stockton Distinguished Scholar-in-Residence at the U.S. Naval War College, NATO Cooperative Cyber Defense Center of Excellence Senior Fellow, and Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas. The Director of the Tallinn Manual 3.0 Project, Schmitt serves on the Department of State's Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts. Follow him on Twitter (@Schmitt_ILaw).

below. Such legal attribution must not be confused with technical attribution, which denotes evidence of the relationship, and from political attribution, which simply refers to a policy decision to blame another state. The foundation laid, the discussion will proceed serially through the various categories of responses existing in international law, zeroing in on the legal preconditions that must exist before engaging in them against a proxy group or the affiliated state.

Two points must be made at the outset. First, "proxy" is not a legal term. Instead, international law asks more specifically about the relationship between the non-state actor and the state concerned. As used in this article, "proxy" simply refers to an individual or group with some link to a state. Whether a proxy's hostile cyber operations are legally attributable to a state depends on the attendant circumstances, which will be outlined below.

Second, the analysis is not limited to Russian use of proxies, for the identity of the state that has resorted to their use is irrelevant in international law pursuant to the principle of sovereign equality. The analysis that follows is as applicable to the use of proxies by states such as China, Iran, and North Korea as it is to Russia.[9]

Unlawful Cyber Operations

The range of lawful response options in the face of proxy cyber operations is determined in part by 1) whether the proxy's operation constitutes an "internationally wrongful act" (unlawful cyber operation) by the affiliated state, 2) whether the victim state's proposed cyber response is unlawful, and 3) the existence of any "circumstances precluding wrongfulness," a legal term of art, that would render lawful the victim state's otherwise unlawful response to the cyber operation directed against it.

There are scores of international law rules that hostile cyber operations, or responses to them, might violate.

The *Tallinn Manual 2.0* project sponsored by the NATO Cooperative Cyber Defence Centre of Excellence identified many.[10] They range from violations of diplomatic or international human rights law to cyber operations that breach the obligations found in the law of the sea, air, or outer space. Excluding violations of the law of armed conflict, three loom large—the obligation to respect the sovereignty of other states, the prohibition on coercive intervention, and the use of force.[11]

Most international law rules, including the three key ones, apply only to states. Although the cyber operations of non-state groups can be criminal acts under the laws of a state that enjoys jurisdiction, without attribution of the cyber operation to a state as a matter of law, there is generally no international law violation. In other words, the question in the proxy context is whether the proxy's operation would breach one of these rules had the state itself conducted it and, if so, whether the proxy's conduct is legally attributable to the state. Before turning to attribution, therefore, the first step is to examine when cyber operations breach international law obligations.

The most likely obligation to be breached by a cyber operation is respect for another state's sovereignty. There has been some controversy regarding whether violation of sovereignty is even a rule of international law, with the United Kingdom suggesting in 2018 that it is not.[12] The United Kingdom argues that a state's remotely-conducted cyber operation into another state's territory does not violate its sovereignty, irrespective of the consequences of the operation; accordingly, neither would a proxy's operation. Since then, every state that has taken a firm stance on the matter accepts the existence of a rule of sovereignty. NATO's Cyber Doctrine even reflects the rule.[13] The US position, however, remains ambiguous.[14] Yet when the United Kingdom issued a "reservation" (a statement of disagreement) regarding NATO's acknowledgment of the rule, the US did not.[15]

From a legal perspective, the better view is that a rule of sovereignty exists. As a general matter, there are two ways a cyber operation can violate sovereignty. First, a cyber operation can do so based on territoriality. This occurs when a state's cyber operation, or a proxy's operation attributable to a state, causes certain effects on another state's territory. Physical damage or injury, as well as permanent loss of functionality, clearly suffice. Whether remotely causing effects that do not reach this level violates sovereignty remains an open question that will only be settled once states publicly begin to set forth their views on the matter.[16] For instance, there is no consensus about whether temporarily interfering with the cyberinfrastructure's functionality or causing it to operate in other than the intended manner qualifies. That said, there is agreement that the rule protects both private and public infrastructure. Additionally, the requisite effects can be caused indirectly. As an example, a cyber operation against a state's COVID-19 management system will violate sovereignty if it results in illness or death that might otherwise have been avoided.[17]

Second, interference with, or usurpation of, an inherently governmental function violates

sovereignty.[18] Inherently governmental functions are those that only a state has the authority to perform. Examples include conducting elections, tax collection, law enforcement, national crisis management, diplomacy, and national defense. Interference occurs when the cyber operation makes it materially more difficult to perform the function, as in temporarily disrupting the operation of election machinery or interfering with defensive military systems like early-warning radars. Usurpation involves performing inherently governmental functions in lieu of the other state, as in conducting law enforcement measures against proxies, such as remote searches or virtual seizure in another state's territory without that state's permission.

Unlike sovereignty, the rule of non-intervention is uncontroversial, with all states accepting its application in the cyber context. Intervention has two elements. First, the cyber operation has to involve a state's internal or external affairs (the so-called *domaine réservé*[19]). These are areas of activity that international law leaves to states to regulate, such as the state's political, economic, and social policies. Second, the hostile cyber operation in question must be coercive in the sense of depriving the victim state of choice by forcing it to (a) adopt a policy it would not otherwise adopt (b) refrain from adopting one it would otherwise adopt or (c) execute a policy in a manner that differs from that intended. Mere persuasion, influence, or diplomatic pressure is insufficient, as are propaganda and most other information operations, even when untruthful. Cyber operations motivated by other than a desire to address policy choice or execution, such as those that are purely criminal, as is often the case with North Korean operations,[20] also do not qualify.

Absent either element, a proxy's cyber operation, whether attributable to a state or not, does not violate the intervention rule (although it might violate other rules, such as sovereignty). For example, it is not intervention to use proxies to engage in an information campaign that benefits a candidate during another state's election, but it would be to have them manipulate election machinery or provide false but believable information as to how to vote online (when online voting is not allowed).[21]

In extreme cases, a proxy's cyber operation that is legally attributable to a state could violate the customary law prohibition on the use of force codified in Article 2(4) of the UN Charter. All states agree that the prohibition applies in the cyber context; the challenge lies in identifying those operations crossing the use of force threshold. And as with the sovereignty and intervention rules, a proxy's cyber operation must be attributable to a state to violate the use of force prohibition. If it is not, it is mere criminality under the domestic laws of states having jurisdiction over the matter.

There is broad agreement that a cyber operation causing physical damage or injury beyond a *de minimis* level amounts to a use of force, as would an operation causing substantial loss of a targeted system's functionality. Below that threshold, consensus among states has proven elusive. Increasingly, they are adopting a case-by-case approach that assesses the "scale and effects" of a cyber operation to determine whether it crosses the use of force line.[22]

The adoption of this approach is significant, for it signals that in the view of these states, there may be proxy cyber operations that are neither destructive nor injurious but that nevertheless qualify as uses of force. France, for example, has taken the position that a cyber campaign resulting in severe nationwide economic disruption could qualify as such, and the Netherlands has hinted that it is willing to come to the same conclusion.[23] By this approach, states will look at an array of non-exclusive factors in deciding whether a proxy's cyber operation is of sufficient scale and if the effects amount to a use of force by the state to which it is attributable. The factors that will be considered include, but are not limited to, the severity of consequences, the geopolitical situation, the track record of the state engaging in the cyber operation, the immediacy and directness of its effects, the entity launching the operation (e.g., military, intelligence, proxy), and the target. However, until states begin to add granularity to their position, the legal character of a particularly severe but non-destructive or injurious cyber operation will remain uncertain.

Importantly, espionage, as such, does not violate international law. Therefore, neither a proxy's cyber espionage nor espionage by a victim state used to fashion a response is unlawful. That said, if the consequences of the espionage qualify as a violation of international law, for instance, because it damages the targeted cyberinfrastructure or is being used for law enforcement purposes (both sovereignty violations), the operation will be unlawful on that basis. Thus, whether a cyber operation has breached an international law obligation is sometimes uncertain. Nevertheless, determining whether a proxy's hostile operation or a state's response to such an operation breaches international law is a necessary first step in identifying lawful response options.

Attribution

The second step in identifying response options is determining whether a proxy's cyber operation is attributable to a state under international law. As explained, establishing international law violations requires both a breach of an international law obligation and attribution of the cyber operation in question to a state (labeled the "responsible state" in international law terms). Only after deciding whether the proxy's operation satisfies both criteria, and whether a particular response by the victim state (the "injured state") would breach any legal obligation itself can the full range of response options for a specific incident be identified.

There are multiple bases for attributing a proxy's cyber operations to a state. To begin with, individuals, groups, or other entities are considered *de facto* organs for purposes of legal attribution if they are completely dependent on the state, as when an intelligence agency creates an unofficial group for the express purpose of conducting hostile cyber operations, funds (perhaps secretly) the group, and determines its operations.[24] In these cases, a proxy is essentially an instrument of the state.[25] Cyber operations are also attributable to a state where individuals, groups, or entities are legally empowered by the state to "exercise elements of governmental authority."[26] The activities must be quintessentially governmental. An example would be

contracting with a private company to perform non-commercial cyber espionage on behalf of the state or conduct offensive cyber operations against the state's adversary.

In both of these situations, even proxy cyber operations that are *ultra vires,* that is, beyond the scope of the authority granted by the state, are attributable to it so long as they are related to the activity. For example, if a company is hired to conduct offensive operations (a quintessential governmental activity) but instructed not to target particular government cyberinfrastructure, yet it nevertheless directs operations against that infrastructure, the state will be responsible for the operations. But if the company engages in classic cybercrime for its own profit, the state will not bear responsibility.

The most common basis for legally attributing proxy cyber operations to a state is when they are conducted "on the instructions of, or under the direction or control of, that state."[27] Acting on a state's instructions generally occurs when a state recruits or instigates a proxy to perform as its "auxiliary" without having any official or legal connection to that state.[28] For instance, the state could recruit a group of volunteer patriotic hackers to supplement its cyber actions, as in conducting espionage that supports the state's hostile operations. As a matter of law, the state would be responsible for the hostile cyber operations conducted by the proxy.

The "direction or control" standard applies when the proxy's affiliation with the state is looser than that of a proxy acting as an auxiliary. In its *Nicaragua* judgment, the International Court of Justice suggested that a proxy's acts are attributable when the state directs or controls specific operations; the Court labeled this "effective control." General support or encouragement of cyber proxy operations is not enough.[29] The Court even held that a state's participation in the "financing, organizing, training, supplying, and equipping" of a proxy organization and "the selection of its military or paramilitary targets, and the planning of the whole of its operation" did not reach the "effective control" threshold.[30] Such involvement in the cyber operations would likely amount to unlawful intervention into the internal affairs of the target state, but the proxy's actions themselves would not be attributable to the state concerned.

Finally, a proxy's cyber operation is attributable as a matter of law to a state when the latter "acknowledges and adopts the conduct in question as its own."[31] The standard requires the state to acknowledge, through words or conduct, that the hostile cyber operation occurred. It must also adopt the proxy's operation by taking affirmative steps to protect or otherwise facilitate its continuation. This happens in very limited situations, for states typically use proxies so they can distance themselves from the hostile cyber operation.

Assessing whether the nature of the relationship between a cyber proxy and a state satisfies the requirements for legal attribution is challenging due to the high thresholds of the various attribution rules and the difficulty of factually establishing the nature of the relationship between the proxy and the state. Complicating matters is the absence of any agreed-upon evidentiary threshold for attribution (unless the case is before a court), disagreement as to whether reasonable but mistaken attribution renders a countermeasure (see below) unlawful, and the

fact that international law does not require states to produce the evidence upon which they base attribution. Nonetheless, only after an attribution determination has been made is it possible to identify the available response options. It is to those options that the discussion turns.

Retorsion and Other Lawful Responses

The most common responses to hostile cyber operations are "acts of retorsion"—unilateral actions that do not violate international law per se, although they are "unfriendly" from the perspective of the entity against which they are directed.[32] Examples include economic sanctions, canceling state visits, expelling diplomats, or even severing diplomatic relations. By way of illustration, when Russia targeted the US with cyber election interference in 2016, including through the use of proxies like the Internet Research Agency, the Obama Administration responded by imposing sanctions, expelling "diplomatic" personnel, and closing Russian facilities in the US.[33] Similarly, the Biden administration has elected to reply to the 2020 Russian election-related cyber operations and the SolarWinds campaign utilizing retorsion.[34]

Retorsion options are an especially useful response to a hostile state or proxy cyber operation that either does not violate international law or is of an ambiguous legal character, as with operations like SolarWinds.[35] Moreover, a state need not legally attribute a proxy's operation to another state before engaging in acts of retorsion against the proxy, its members, or a state it suspects of involvement; it even would be lawful to sanction them based on mere suspicion of involvement, assuming doing so is compliant with the state's domestic law. Simply put, acts of retorsion are always available response options because they are lawful measures unconstrained by the international legal requirements that accompany more robust self-help measures discussed below. Of course, a responsible member of the international community should only engage in retorsion when reasonable in the circumstances and in good faith.

Economic sanctions are a prominent means of retorsion and a core element of US strategy to deter Russia's use of cyber proxies and other malicious behavior. The US generally relies on Executive Order (EO) 13694 as amended by EO 13757, which was codified in the Countering America's Adversaries Through Sanctions Act (CAATSA), to sanction Russians and Russian entities that have engaged in hostile cyber operations.[36] Section 224 of CAATSA expressly authorizes sanctions against cyber proxy operations conducted on behalf of the Russian government that undermine "cybersecurity against any person, including a democratic institution, or government."[37] Hundreds of proxy group members and Russian security and intelligence services personnel have been sanctioned for having conducted cyber operations using these authorities.[38]

Cyber responses that do not cause effects that would violate international law also qualify as acts of retorsion. For instance, a state targeted by a proxy's cyber operations may undertake cyber information (and even disinformation) campaigns,[39] cyber espionage, and other intelligence and counterintelligence cyber operations against both a proxy or a state with some

relationship to the hostile operations, so long as the cyber responses do not cross any legal threshold, such as those described above, that would render them unlawful.[40] Or a targeted state could establish access within hostile cyberinfrastructure without causing internationally wrongful effects to signal its capability and willingness to respond to future hostile cyber operations.[41] The victim state could even block access by proxy groups, individuals, and specified states to its cyberinfrastructure as an act of retorsion, for there is no international law right of access to cyberinfrastructure on another state's territory.[42]

Other lawful means of responding to proxy cyber operations are available. For instance, the United States is increasingly resorting to judicial action by indicting members of proxy groups for domestic criminal offenses, as in the case of the Yahoo data breach mentioned above[43] and a 2019 criminal indictment of two members of Evil Corp, a Russian-based cybercriminal organization accused of supporting the Russian government's hostile cyber efforts.[44] The targeted state can also seek a UN Charter, Chapter VII, Security Council resolution condemning proxy operations and authorizing interference, disruption, or even destruction of a proxy's cyber capabilities, as well as sanctions or other action against a state supporting the group.[45] Of course, doing so in the case of Russia or China would be impossible in light of their veto power as one of the permanent five (P5) members of the Security Council. Judicial action in the International Court of Justice against a state to which a proxy's operations are attributable is a theoretical possibility, although highly unlikely because of the jurisdictional hurdles of bringing another state before that court.[46]

States are inclined to resort to the retorsion option or judicial action to respond to hostile proxy cyber operations, not only because they are a lawful option when reacting to hostile cyber operations that do not violate international law, but they also minimize political and legal risk in situations where there is uncertainty as to whether the proxy's cyber operation is unlawful. Moreover, factual evidence of attribution may be difficult to acquire, or the legal threshold for attribution may not have been reached in a case where a foreign state's involvement is suspected. Conducting acts of retorsion against that state is nevertheless permissible, while most other self-help measures would not be. Such measures may prove inadequate, however, in limiting or deterring the use of cyber proxies, for they generally impose limited repercussions, thereby necessitating an understanding of other measures of self-help.

Countermeasures

In certain circumstances, a state might need to take more robust measures—such as countermeasures, actions undertaken out of necessity, or self-defense—in the face of proxy cyber operations. Each of these responses would otherwise violate international law, but international law treats them as "circumstances precluding wrongfulness."[47] In other words, responses against the responsible state in the underlying circumstances are justified or excused under international law even though they are technically unlawful acts, so long as strict legal criteria for each are met, as we will discuss below.

Countermeasures are otherwise unlawful actions that international law nevertheless allows an injured state to take to compel a responsible state to stop its unlawful conduct or to provide reparations (including compensation) for any harm caused.[48] For example, an injured state may respond to the proxy's unlawful cyber operation with its own cyber operation that violates the sovereignty of a state responsible for a proxy's operations. The operation could even take the form of a violation of the responsible state's sovereignty by conducting operations against the proxy's cyberinfrastructure on the responsible state's territory.

Countermeasures are by definition violations of international law, they are subject to stringent limitations. First, they are only available against hostile cyber operations that are internationally wrongful acts. In the proxy context, that means the proxy's hostile cyber operation must breach an international law rule and be legally attributable to a state before countermeasures are on the table. In the event of misattribution, the prevailing view is that the purported countermeasure is itself unlawful because there was no "circumstance" to "preclude its wrongfulness."[49]

Additionally, a desire to retaliate against the state to which the proxy's operations are attributable cannot be the predominant motivation for countermeasures; the primary purpose instead must be to directly terminate the hostile cyber operations or influence the responsible state to end the proxy's cyber operations (or provide reparations). This being so, cyber responses unlikely to end the proxy's hostile operations or cause the responsible state to offer reparations do not qualify as countermeasures; they are unlawful. Further, since countermeasures are meant to return a situation to one of compliance with international law, they are only available while the responsible state's unlawful cyber operation (including by a proxy), is underway. For the same reason, a state may not take them once that operation or a series of related unlawful operations (a cyber campaign) are complete.

Countermeasures also must be proportionate in the sense that they have to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[50] In other words, the pain inflicted on the responsible state by the state taking the countermeasure must be roughly equal in scope and severity to that suffered as a result of the former's operations or those of its proxy. Further, it is now well accepted that countermeasures may not involve the use of force; only non-forcible measures are permitted as countermeasures.[51]

Several issues surrounding countermeasures remain unsettled in law. For instance, there is no consensus about whether an injured state has a legal obligation to attempt lesser measures, such as cyber retorsion or countermeasures with less severe consequences, before employing countermeasures. Most of the *Tallinn Manual 2.0* experts believed that no such obligation exists, but it remains an open issue.[52] There is also a degree of uncertainty about when an injured state must notify the responsible state that it intends to take countermeasures. Generally, notification must precede the taking of countermeasures unless they are urgent.[53] In the

cyber context, states have been interpreting this exception very broadly because of the speed with which cyber operations unfold and the fact that notice may provide an adversary critical information regarding the injured state's cyber capabilities.[54] Yet, in fairness, advance notice makes some sense in the cyber proxy context, where there may be intentional efforts to spoof or mask origin and affiliation with a state. Notice would allow the state against which countermeasures are to be taken to offer evidence that it is not responsible for the proxy's operations, perhaps even by cooperating with the targeted state. The best view, and one balancing the interests of states, is that notice should not be required if infeasible in the circumstances.

The most significant unsettled issue is whether collective countermeasures are permissible, much like the UN Charter and customary law permit collective defense in response to an armed attack.[55] The question is whether a state targeted by a proxy's unlawful cyber operation that is attributable to another state may look to third states for help in conducting countermeasures, either by assisting or by engaging in countermeasures on behalf of the injured state. States are split (or non-committal) on the issue. For instance, Estonia takes the position, understandably in light of its vulnerability to hostile cyber operations by Russia and its proxies, that it may seek help from other states in taking countermeasures; NATO-ally France takes the opposite position.[56] As a matter of law, the better position is that collective countermeasures are permissible, but the paucity of state views on the matter means it remains an open question.[57]

Several illustrations are helpful to explain the taking of countermeasures. For cyber proxy operations originating from within another state's territory, countermeasures could consist of "hack backs" or other cyber responses targeting the source of the initial hostile operation. Suppose a hacker group located in and acting on state A's instructions is the source of a hostile cyber operation causing loss of functionality of private cyberinfrastructure in state B (a violation of its sovereignty). In that case, the latter may target the private hacker group's cyberinfrastructure in state A to shut it down. The operation would otherwise violate that state's sovereignty, but its wrongfulness is precluded by its status as a proportionate countermeasure.

However, countermeasures need not be directed at the source of the initial cyber operation. They may proportionately target any cyberinfrastructure located within the state to which the proxy's operations are attributable, whether government or privately-owned, to influence the responsible state to compel its proxy to desist (or to secure reparations from that state). The response need not even violate the same legal obligation. For instance, a proxy's attributable cyber operation against private cyberinfrastructure that violates another state's sovereignty could be responded to through cyber operations against the responsible state's satellites in a manner that contravenes space law. Similarly, non-cyber countermeasures (like the denial of landing rights provided for in a treaty or the closure of the territorial sea to "innocent passage" by the state's vessels) are permissible in the face of unlawful cyber operations (and vice-versa).[58]

Cyber proxies do not always operate from within the territory of the state to which their operations are attributable. When proxies operate from a third state, the injured state may employ

countermeasures directed at targets located in the responsible state's territory. A targeted state might, however, prefer to take action against the proxy's operations in the third state. The legal problem is that countermeasures may only be directed against a state that has breached a legal obligation owed to the state taking the countermeasures. Since countermeasures are otherwise unlawful actions, they would seem to be unlawful vis-à-vis the territorial state. The remedy to this situation can sometimes be found in the rule of due diligence.[59] States either disagree on the existence of such a rule or have not opined on its existence.[60] Nevertheless, the weight of opinion is that such a rule exists and is of particular relevance in the cyber context.

By it, states must put an end to ongoing cyber operations either mounted from or conducted remotely through cyberinfrastructure located on their territory whenever it is feasible for them to do so in circumstances where the operations are causing "serious adverse consequences" for a legal right of another state (such as sovereignty). This obligation does not require that the hostile cyber operation be legally attributable to a state, although it may be. And this is crucial because if a state uses a proxy from its own or another state's territory, but attribution cannot be established or the relationship does not reach the legal threshold for attribution, the due diligence rule may open the door to countermeasures.

To illustrate, assume cyber proxies are operating from one (territorial) state to intervene in the target state's elections unlawfully. The territorial state knows of the operations and can stop them. Yet, it fails to do so because it sympathizes with the proxy group, is allied with the responsible state, or for any other reason. The territorial state is in breach of its due diligence obligation. The injured state may take countermeasures against the territorial state to convince it to comply with its due diligence obligation to end the proxy's operations or even conduct operations against the proxy itself. In such a situation, the injured state's otherwise unlawful action (perhaps a breach of sovereignty) would be precluded because it qualifies as a countermeasure against the territorial state's non-compliance with the rule of due diligence.

A significant issue here is how to interpret the requirement that the taking of action be feasible before the due diligence obligation is breached. In this regard, the territorial state need only look to its own capabilities, such as technical solutions, classic law enforcement, instructing an Internet Service Provider to terminate service to the proxy, or even retaining the services of a private company that can terminate the proxy's operations. However, it need not accept assistance from the injured or other states; feasibility is assessed based on the state's capabilities alone.[61]

Actions Taken Out of Necessity

Targeted states may not have the option of employing countermeasures because the proxy's cyber operation does not violate international law, attribution cannot be established, or it is not feasible for the territorial state to terminate the proxy's operation and is therefore not in breach of any due diligence obligation. In these situations, the targeted state may take action based on a plea of necessity.

Plea of necessity actions are similar to countermeasures in that a state targeted by certain hostile cyber operations is permitted to respond in a manner that would otherwise violate international law; it is a "circumstance precluding the wrongfulness" of the response. States may do so in exceptional situations where cyber operations, including those mounted by proxies, create a "grave and imminent peril" to an "essential interest" of the targeted state, and the proposed response is the sole means of addressing the situation.[62]

Unlike countermeasures, the hostile cyber operation need not constitute an internationally wrongful act. This has two significant consequences. First, a hostile cyber operation does not have to breach any particular obligation of a state. Thus, uncertainty about whether a hostile cyber operation breaches an obligation such as respect for sovereignty or refraining from intervention, or certainty that it does not, is no obstacle to acting based on necessity.

Second, in the proxy context, unlike in regards to countermeasures, it is unnecessary to legally attribute the hostile cyber operation to a state before responding based on necessity. Indeed, there is no requirement to attribute the cyber operation to any particular entity at all. The sole requirement is a factual determination that the cyber operation, irrespective of who might have launched it, gravely threatens an essential interest of the targeted state, and the proposed response is the only feasible means to prevent or end the intrusion.

For instance, consider a proxy cyber operation targeting essential cyberinfrastructure, such as the national financial system, launched from a state to which attribution is suspected but cannot be established. Furthermore, the state might not be in breach of its due diligence obligation because it is uncertain whether it has the ability to put an end to the operation. The targeted state's proposed response would otherwise violate, at minimum, the territorial state's sovereignty. Yet, in this situation, the unlawfulness of that response would be precluded so long as the narrow criteria for the plea of necessity are satisfied.

The hostile cyber operation must be grave and imminent before the targeted state may respond. "Grave" denotes a threatened or ongoing hostile operation with consequences that are exceptionally severe, detrimental, or have an otherwise acute impact on an essential interest of the state. A proxy's operation that targets an essential interest with only a limited effect would fall short of this standard. "Imminent" indicates that a targeted state is allowed to respond anticipatorily. Imminence is not to be understood in terms of time. Rather, a threat is imminent where failure to respond would deprive the state of the opportunity to prevent or stop the proxy's hostile cyber operation effectively.[63]

In addition, an essential interest must be affected. Unfortunately, international law does not define the term. The *Tallinn Manual 2.0* experts describe it as an interest "that is of a fundamental and great importance to the State concerned."[64] Certain areas of activity are clearly essential to all states. Paradigmatic examples include national economic well-being, public health and safety, communications, power generation, and national security. Notably, a state's designation of cyberinfrastructure as critical does not definitively mean it qualifies as essential in international law terms.

Moreover, what is essential is a contextual determination. For instance, in all countries, the economic health of the nation is essential. But while tourism drives the nation's economic well-being for some countries, in others it is economically incidental. Accordingly, proxy cyber operations targeting the tourism industry in the former countries might qualify as directed at an essential interest, but not in the latter ones.

A proxy group targeting an essential interest is not enough to warrant otherwise unlawful responses; the additional criteria must be satisfied. Key among these is that the otherwise unlawful operation is the only feasible course of action for putting an end to the grave and imminent peril. If lesser response measures such as acts of retorsion or switching to a secondary or backup system, can safeguard the interest, a targeted state may not act out of necessity.

A state responding in a situation of necessity must be cautious when its response could cause effects on the territory of a state or states from which the proxy's cyber operations either do not originate or to which they cannot be attributed in law. Given the complex and interconnective nature of cyberinfrastructure, these situations present themselves with some frequency. A limiting factor in this regard is that a targeted state must assess whether its response will seriously impair the essential interests of other states.[65] If so, it may not act out of necessity regardless of the magnitude of the harm it is enduring.

Self-Defense

In extreme circumstances, a state may need to respond with use of force level measures to end proxy cyber operations. As noted, countermeasures may not involve the use of force,[66] while whether the plea of necessity allows for a force level response remains unsettled.[67] A state in this situation has three options—consent from the state into which the operations are to be conducted, a UN Security Council resolution authorizing the action, or self-defense. Consent or adoption of a Security Council resolution is unlikely in the case of Russian or Chinese-linked proxy cyber operations, as they would not approve of using cyber force on their territory, and they could use their status as permanent members of the Security Council to veto any resolution authorizing responses at the use of force level. As a consequence, some proxy cyber operations may only be responded to on the basis of the right to self-defense.

Article 51 of the UN Charter, which reflects customary international law, provides "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." That states may use force in self-defense against a cyber armed attack is self-evident. The question is when and how a cyber operation qualifies as an armed attack against which force, whether cyber or kinetic, may be used.

States agree that cyber operations that cause significant physical damage, destruction, death, or injury are armed attacks.[68] Whether those causing a lesser degree of damage or injury, or non-destructive or injurious harm, may be characterized as armed attacks remains an open

debate, but France has gone as far as indicating that a non-destructive cyber operation against its national economy might even qualify.[69] States that have spoken on the issue increasingly agree with the International Court of Justice that whether a non-destructive cyber operation is a use of force at the armed attack depends on its "scale and effects."[70] Precisely where the threshold lies, however, remains unresolved.

The right to act in self-defense is subject to two requirements, necessity and proportionality.[71] Necessity in this context requires a situation in which the targeted state must use cyber or kinetic force to prevent the cyber armed attack, should it be imminent, or to defeat it if the attack is underway. Proportionality limits the degree of force to be used to only that which is required to defeat the imminent or ongoing armed attack effectively.

In the proxy context, two contentious issues loom large. The first is attribution. There is consensus that the targeted state may use force in self-defense against a state or a proxy group if the proxy's cyber armed attack is conducted on behalf of that state or with its "substantial involvement" in the operations.[72] The law is unsettled, however, for situations where a proxy's cyber operation is not attributable to a state either due to insufficient evidence that the operation is being mounted on behalf of the state or because a state's involvement is not substantial. A majority of the *Tallinn Manual 2.0* experts and some states, including the United States, support the view that attribution is not necessary to qualify a proxy cyber operation as an armed attack. A non-attributable cyber operation at the armed attack level also triggers the targeted state's right to respond in self-defense.[73] This is the better position, for if a proxy's operation cannot qualify as an armed attack unless attributable to a state, targeted states would be limited to non-forceful response options—acts of retorsion, countermeasures, or actions out of necessity—to defeat the most severe cyber operations by cyber proxies. In some cases, such a response would prove insufficient.

Assuming that a proxy's cyber operation may qualify as an armed attack without attributing the conduct to a state, controversy also exists around whether a forcible defensive response against the proxy is allowed into a state to which the operation cannot be attributed. A majority of the *Tallinn Manual 2.0* experts support the position, one shared by the United States, that a targeted state may respond with force that is both necessary and proportionate against the proxy so long as the state is unable or unwilling to stop the proxy's cyber armed attack.[74] Take the case of a cyber proxy conducting operations from state A's territory that cause significant damage to state B's critical cyberinfrastructure. The targeted state believes state A is behind the operation but cannot acquire sufficient evidence to attribute the operations confidently. If it cannot be established that state A is able and willing to stop the operations, the targeted state may employ necessary and proportionate cyber operations at the use of force level against the cyber proxy in state A. The same would apply to cyber proxies operating within other states that are not linked to the proxies so long as those other states are unable and unwilling to stop the proxy.

CONCLUSION

The use of cyber proxies by states like Russia, China, North Korea, and Iran adds a layer of complexity to the legal and policy assessments that targeted states must make when considering how to respond to hostile cyber operations. In particular, the factual and legal relationships between a proxy and the state concerned may determine whether particular types of responses against proxy cyber operations are permissible. Nevertheless, in certain circumstances, international law allows for meaningful responses even when attribution to a state is uncertain or altogether missing.

The critical point to grasp is that the international law governing response options is often permissive in terms of allowing responses, but at the same time, can be very nuanced and even unsettled. Thus, every situation merits granular analysis when deciding how to limit, stop, and deter hostile cyber operations by cyber proxies. Over time, state practice in dealing with proxy cyber operations combined with statements from states regarding how they interpret the relevant international law will yield greater clarity on the options available to defeat and deter hostile proxy cyber operations.

NOTES

1. Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online* 42, no. 1 (August 2017): 1-4, https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf.
2. This point was made by the last administration but remains valid today. The White House, National Security Strategy of the United States of America (Washington, DC, December 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; Department of Defense, Summary of the National Defense Strategy (Washington, DC, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
3. United Nations General Assembly, Sixty-Eighth Session, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, June 24, 2013, ¶ 23, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf.
4. Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010), 23-24.
5. U.S. Congress, Senate, Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 116th Congress, 1st Session, S. Rep. 116-290, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.
6. U.S. Department of Justice, Office of Public Affairs, U.S. *Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
7. National Intelligence Council, *Foreign Threats to the 2020 US Federal Elections*, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
8. Steve Cunningham, *Key Strategic Issues List (KSIL) 2021-2022* (Carlisle Barracks, PA: U.S. Army War College Press, 2020), https://press.armywarcollege.edu/monographs/906.
9. On China, see Cybersecurity and Infrastructure Security Agency, *Potential for China Cyber Response to Heightened U.S.–China Tensions*, Alert AA20-275A, October 1, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-275a; on Iran, see Catherine Theohary, U.S. Library of Congress, Congressional Research Service, *Iranian Offensive Cyber Atttack Capabilities*, IF11406, January 13, 2020, 1; on North Korea, see Cybersecurity and Infrastructure Security Agency, *AppleJeus: Analysis of North Korea's Cryptocurrency Malware*, Alert AA21-048A, February 17, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-048a.
10. See Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).
11. Schmitt, rules 1, 66 and 68 respectively.
12. Jeremy Wright, Attorney General, United Kingdom, "Cyber and International Law in the 21st Century," *Chatham House*, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
13. NATO, Ministry of Defence, AJP–3.20 (ed. A, v. 1), *Allied Joint Doctrine for Cyberspace Operations* (2020), ¶ 3.7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
14. See Michael Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace," *Just Security*, March 11, 2020, https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.
15. See AJP–3.20, v.
16. Republic of France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019), § 1.1.1, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf; Finland, Ministry of Foreign Affairs, *International Law and Cyberspace: Finland's National Positions*, October 15, 2020, 1-3, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c-6d85?t=1603097522727; Federal Republic of Germany, Ministry of Defense, *On the Application of International Law to Cyberspace*, March 2021, 2-4, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf. France, Finland, and Germany are the only three states that have proffered their view.
17. Marko Milanovic and Michael N. Schmitt, "Cyber Attacks and Cyber (Mis)information Operations During a Pandemic," *Journal of National Security Law & Policy* vol. 11, no. 1, October 19, 2020, 252–54, https://jnslp.com/wp-content/uploads/2020/12/Cyber-Attacks-and-Cyber-Misinformation-Operations-During-a-Pandemic_2.pdf.

NOTES

18. Schmitt, ed., *Tallinn Manual 2.0*, 22-23.
19. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Judgment, 1986 I.C.J. Rep. 14, ¶¶ 202, 205 (1986); Schmitt, ed., *Tallinn Manual 2.0,* rule 66.
20. U.S. Departments of State, the Treasury, Homeland Security, and the Federal Bureau of Investigation, DPRK Cyber Threat Advisory, *Guidance on the North Korean Cyber Threat,* April 15, 2020, https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.
21. Michael N. Schmitt, "Foreign Cyber Interference in Elections," *International Law Studies* 97, 739 (March 2021): 744-50, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2969&context=ils.
22. See Schmitt, ed., Tallinn Manual 2.0, 333-37; France, *Operations in Cyberspace,* § 1.1.2; Germany, *International Law to Cyberspace,* 6; Finland, *International Law and Cyberspace,* 6-7; Kingdom of Netherlands, [Letter from the] Minister of Foreign Affairs to the President of the House of Representatives, *Appendix: International law in cyberspace,* July 5, 2019, 4, https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf; Government of Australia, Australia's International Cyber Engagement Strategy, *Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace* (2017), https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html; NATO, AJP–3.20, ¶ 3.7.
23. See France, *Operations in Cyberspace,* § 1.2.1. France has, in fact, stated such economic damage may rise to the level of an armed attack. Netherlands, International law in cyberspace, 4.
24. *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 2007, I.C.J. Rep. 43, ¶ 392 (2007); *Nicaragua*, 1986 Judgment, ¶¶ 109-10.
25. *Bosnia*, 2007 Judgment, ¶ 392.
26. International Law Commission, fifty-third session, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10, November 2001, art. 5.
27. *Articles on Responsibility of States*, art. 8.
28. *Articles on Responsibility of States,* art. 8, ¶ 2.
29. *Nicaragua,* 1986 Judgment, ¶ 115; *Articles on Responsibility of States*, art. 8, ¶¶ 4-5, Schmitt, ed., *Tallinn Manual 2.0*, rule 17.
30. *Nicaragua*, 1986 Judgment, ¶ 115.
31. *Articles on Responsibility of States*, art. 11; Schmitt, ed., *Tallinn Manual 2.0*, rule 17.
32. Thomas Geigrich, "Retorsion," in *Max Planck Encyclopedia of Public International Law* (Oxford, UK: Oxford University Press, 2011), § 1-3.
33. David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *The New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.
34. David E. Sanger and Andrew E. Kramer, "U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation," T*he New York Times,* April 15, 2020, https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html.
35. Michael N. Schmitt, "Top Expert Backgrounder: Russia's SolarWinds Operation and International Law," *Just Security,* December 21, 2020, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
36. U.S. Department of Commerce, International Trade Administration, *Overview of United States sanctions on Russian persons (individuals, entities, and vessels*), November 12, 2020, https://www.trade.gov/knowledge-product/russia-sanctions.
37. Countering America's Adversaries Through Sanctions Act, 22 U.S.C. § 9524 (2017).
38. U.S. Department of Treasury, Office of Foreign Assets Control, Sanctions List Search, https://sanctionssearchofac.treas.gov/ (last accessed on April 29, 2021).
39. Schmitt, ed., *Tallinn Manual 2.0*, rule 26.
40. Schmitt, ed., *Tallinn Manual 2.0,* rule 32.
41. Robert Chesney, "The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes," *Lawfare,* September 25, 2018, https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

NOTES

42. Schmitt, ed., *Tallinn Manual 2.0,* rule 2.
43. U.S. Department of Justice, *U.S. Charges Russian FSB Officers.*
44. U.S. Department of Treasury, Press Release, *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware,* December 5, 2019, https://home.treasury.gov/news/press-releases/sm845.
45. Schmitt, ed., *Tallinn Manual 2.0,* rule 76.
46. Statute of the International Court of Justice, art. 36, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 145.
47. *Articles on Responsibility of States,* chapter V.
48. *Articles on Responsibility of States,* art. 49; Schmitt, ed., *Tallinn Manual 2.0,* rule 21.
49. Schmitt, ed., *Tallinn Manual 2.0,* 131-32.
50. *Articles on Responsibility of States,* art. 51; Schmitt, ed., *Tallinn Manual 2.0,* rule 23.
51. *Articles on Responsibility of States,* art. 50(1)(a), ¶ 5; Schmitt, ed., *Tallinn Manual 2.0,* rule 22.
52. Schmitt, ed., *Tallinn Manual 2.0,* rule 21, ¶¶ 4, 9.
53. *Articles on Responsibility of States,* art. 52, ¶ 6.
54. See, e.g., France, *Operations in Cyberspace,* § 1.1.3; Netherlands, *International law in cyberspace,* 7; Wright, "Cyber and International Law;" Schmitt, ed., *Tallinn Manual 2.0,* rule 21, ¶¶ 10–12.
55. UN Charter, art. 51.
56. Kersti Kaljulaid, President of Estonia, *Opening of CyCon 2019,* May 29, 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html; cf. France, *Operations in Cyberspace,* § 1.1.3.
57. Michael N. Schmitt and Sean Watts, "Collective Cyber Countermeasures?" *Harvard National Security Journal* (forthcoming).
58. It should be cautioned that this definition of proportionality differs from that in other bodies of law, such as self-defense, human rights, and the law of armed conflict.
59. Schmitt, ed., *Tallinn Manual 2.0,* rule 6.
60. See Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *Yale Law Journal* 125 (2015): 68-81.
61. Schmitt, ed., *Tallinn Manual 2.0,* 49-50.
62. *Articles on Responsibility of States,* art. 25(1)(a); Schmitt, ed., *Tallinn Manual 2.0,* rule 26.
63. Schmitt, ed., Tallinn Manual 2.0, 139*; Case Concerning the Gabčíkovo-Nagymaros Project (Hungary/Slovakia),* Judgment, 1997 I.C.J. Rep 7. ¶ 54 (1997).
64. Schmitt, ed., *Tallinn Manual 2.0,* 135.
65. *Articles on Responsibility of States,* art. 25(1)(b); Schmitt, ed., *Tallinn Manual 2.0,* 137.
66. *Articles on Responsibility of States,* art. 50(1)(a), ¶ 5; Schmitt, ed., *Tallinn Manual 2.0,* rule 22.
67. Schmitt, ed., *Tallinn Manual 2.0,* rule 26, ¶¶ 18–19*; Articles on Responsibility of States,* art. 25, ¶ 21.
68. Schmitt, ed., *Tallinn Manual 2.0,* 341.
69. France, Operations in Cyberspace, § 1.2.1.
70. Nicaragua, 1986 Judgment, ¶ 195.
71. Schmitt, ed., *Tallinn Manual 2.0,* rule 72.
72. Nicaragua, 1986 Judgment, ¶ 195; Schmitt, ed., *Tallinn Manual 2.0,* rule 71, ¶¶ 16-17.
73. Schmitt, ed., *Tallinn Manual 2.0,* rule 71, ¶¶ 19-20; U.S. Department of Defense, *Law of War Manual* (June 2015,updated December 2016), § 16.3.3.4.
74. Schmitt, ed., *Tallinn Manual 2.0,* rule 71, ¶¶ 25-26; *Law of War Manual,* § 17.18.2.

The Cyber Defense Review

Professional Commentary

Toward a Zero Trust Architecture Implementation in a University Environment

Erik Dean
Shane Fonyi
Lieutenant Colonel Christopher Morrell, Ph.D.
Dr. Michael Lanham
Colonel Edward Teague, Ph.D.

ABSTRACT

The core concepts of Zero Trust Architecture have existed since the Jericho Forum in 1994 and have served as the goal of cyber security specialists for many years. Zero Trust Networks and Architectures are extremely appealing to institutions of higher learning because they offer the flexibility to support research and learning while protecting resources with different protection levels, depending on the sensitivity of the resource. This paper investigates how other universities can employ the Zero Trust Architectures using the West Point model.

INTRODUCTION

Traditional network architectures focus on a static defensive perimeter augmented by multiple static layers of additional security which are more than sufficient when resources within the perimeter remain in fixed locations with a user population located within the same perimeter. With more mobile users it does not work, especially as cloud computing becomes more prevalent. These new circumstances require

Erik Dean is the Chief of Information Technology and Security Operations at the Army Cyber Institute. He conducts research in emerging technology implementation and integration. He has previously worked for the Office of Economic and Manpower Analysis and the Information Technology Operations Center. Mr. Dean has a background in Computer Science, Criminal Justice, and Network Technologies.

organizations to adapt policies and procedures to fit them. Organizational control and security over data stored in the cloud and accessible from the internet is generally more difficult on networks with only on-premises controls. Once data leave a physical location, networks with traditional policies and procedures are often unable to secure that data from unauthorized party access. The same goes for devices that connect back to the network using legitimate credentials without sufficient scrutiny of that connecting device. Exclusive focus on the user and security of the credentials exposes the device to compromise even with necessary protections in place, such as multi-factor authentication. Zero Trust Architecture (ZTA) is not only about technical controls to prevent unauthorized access, but also about policies that promote a more secure and mobile workforce. The concept of defense in depth is the main principle in focus for this architecture type, but now with a greater focus on endpoints outside the network perimeter.

With ZTA, there is an assumption that there is no inherent trust between two assets. All connections are scrutinized as if they were previously unknown. Authentication and authorization are separate functions that must occur before a session can be established with an enterprise resource.[1] When a user attempts to connect to a resource from any device or network, the user must be authenticated, the device must be trusted, the resource must be verified, and finally the authorization for access to the resource must be validated. Only after the Zero Trust workflow is completed, can a session be allowed, and the user given access to the data. The concept differs from traditional networks that automatically trust all connections within the internal network enclave without scrutinizing the endpoints making the connections. If the network traffic is allowed, then the session will be established in most instances. This will require organizations to confirm that their controls and policies currently address these topics and can adapt to the changing environments.

Shane Fonyi is a Cybersecurity Analyst for The United States Military Academy at West Point. He is responsible for responding to and preventing cyber incidents at the Academy as well as the engineering and maintenance of the IT security systems currently in place. Prior to that, he was a Cyber Research Integrator for the Army Cyber Institute at West Point and a Security Engineer at The University of Kansas (KU). He has been a speaker at several IT and information security conferences including the International Conference on Cyber Conflict, BSides KC, and the Conference on Higher Education in Kansas for work involved in 5G security, IoT research, and security awareness. He currently holds a Bachelor of Science in Electrical Engineering from KU as well as several industry certifications including the CISSP, CySA+, GMON, GCFA, and SSCP. He is also an NYU Cyber Fellow at the NYU Tandon School of Engineering.

Some organizations have implemented bring-your-own-device (BYOD) programs, but many of those still have major organizational security concerns, and few as yet have solutions.[1] This paper addresses the National Institute of Standards and Technology (NIST) recommendations for implementing Zero Trust Architectures,[2] from both a policy and a technical perspective, and how the NIST recommendations might apply to University networks that track the West Point network as an example.

BACKGROUND

In early 2018, DoD and US Military Academy (USMA) leadership determined that the network security paradigm applied to traditional DoD networks was insufficient to allow USMA cadets and faculty to foster the kind of academic rigor required of one of the nation's top educational institutions. The decision was made to transition the USMA network and architecture to a design more closely aligned with those found at other academic institutions, to include a Zero Trust Architecture that provides an equivalent level of security mandated by DoD while ensuring the flexibility demanded by academic research and education.

DATA AND COMPUTE AS RESOURCES

As an institution of higher learning, the U.S. Military Academy has a broad range of technological and data resources that were considered for inclusion into the Zero Trust Architecture. This breadth of data and resources is compounded by the fact that USMA is also a DoD asset and has other resources not common to other universities. These resources were considered for inclusion based on their access to the West Point Research and Education Network (WREN). In this case, the selection criteria were simple in that the resources were included in the assessment only if the resource in question can be accessed by WREN users or utilize the WREN for network transport.

Lieutenant Colonel Christopher Morrell is an Associate Professor and the Director of the Cyber Science Program within the Electrical Engineering and Computer Science Department, U.S. Military Academy, West Point, NY. He holds a Ph.D. from Virginia Tech where he studied Moving Target Defense using IPv6. His research interests include network security and optimization, network management, and mobile device software development. Email: christopher.morrell@westpoint.edu.

After considering all devices and data sources that use WREN to transport or process, the following categories were used as resource groups to determine access levels during the dynamic access and authorization steps discussed below, as follows:

1) Personally-owned devices with no health, security configuration, or compliance checking.

2) Enterprise-owned devices and systems that do not support network-based authentication. These devices require network transport and some level of WREN resource connectivity, but configuration and compliance cannot be checked automatically. This category of resources and devices may present a higher risk to other WREN resources.

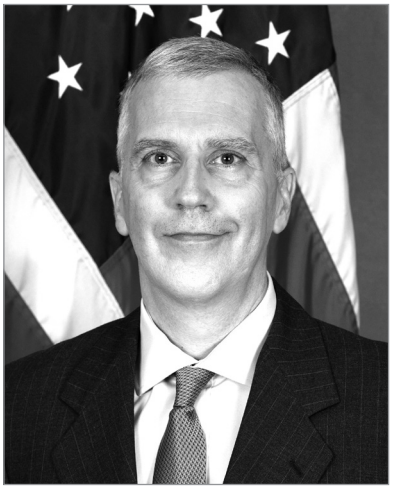
3) Devices able to (a) perform automated health and security policy compliance checks, (b) be integrated with the device management solution chosen, and (c) perform challenge/response authentication at the network level.

4) Systems, devices, or applications that contain or process Personal Health Information (PHI) or medium-to-large volumes of Personally Identifiable Information (PII), whether or not able to perform challenge/response authentication or report device health/configuration information. These require the highest level of protection.

These categories apply to data contained both within Information Systems (ISs) and the devices.

COMMUNICATIONS SECURED BY NETWORK LOCATION

By design, WREN resources generally must be accessible from anywhere on the planet. As with most contemporary top-tier universities, several West Point cadets participate in immersive study programs, and travel abroad, as is true with West Point staff and faculty, and all require continuous access to WREN resources. Frequent travel is common for most universities,



Dr. Michael Lanham is an Associate Professor with the Department of Electrical Engineering and Computer Science (EECS) and Chief Information Security Officer (CISO) of the United States Military Academy (USMA). Michael served 27 years in the Army, culminating as an Academy Professor at USMA with EECS. Prior to that he was a FA53 - Information Systems Management officer since 2003. LTC Lanham was commissioned into the Infantry in 1992 from North Carolina State University. He has served in numerous deployments to Macedonia, Bosnia-Herzegovina, Sierra Leone, Liberia, and Kuwait. His military assignments included duty with 2-15 Infantry Regiment, 3rd Infantry Division (Mechanized) (Schweinfurt, Germany) and Special Operations Command Europe (SOCEUR) (Stuttgart, Germany) as well as with the 1st Brigade and D Co/1-327 Infantry Regiment, 101st Airborne Division (Air Assault) (Fort Campbell, Kentucky). He has also served as faculty at USMA, in various staff positions with USSTRATCOM, Joint Functional Component Command (JFCC)-Integrated Missile Defense (IMD), JFCC-Network Warfare (JFCC-NW), USARCENT, USASMDC/ARSTRAT/ARFORCYBER, and ARCYBER.

which creates challenges for restricting communications based on location and can significantly degrade end-user services. The NIST recommendation therefore would seriously impact user's ability to do their jobs.

Due to these factors, most WREN resources are not restricted by location. The security tools embedded in cloud computing platforms like Google Workspace and Microsoft Office 365 enable this. WREN's cyber security staff leverage the advanced threat identification and mitigation tools these platforms have, in order to compensate for the inability to restrict by geographic location or network location.

While generally unrestricted, there are network controls and restricted access within the fourth category of resources above, which apply only to the local West Point network enclave and do not need external location access. These resources are restricted to on-premises users whose devices meet all requirements for authentication and device health attestation and validation, facilitated by multiple mechanisms such as geographic location via the Company Portal device management platform, client-provided network address (also identified through the Company Portal software), and, finally, the network group to which the device and user have been assigned. If the user and device are trusted, meet all compliance criteria, and are either geographically or logically, though some remote access mechanism such as virtual private networking (VPN), located at West Point, they can access those restricted resources.

WREN takes this requirement further than traditional networks with Software Defined Network (SDN) and the capabilities it provides.

ACCESS GRANTED ON PER-SESSION BASIS

Authorized users with personal and enterprise-owned devices gain access to WREN resources primarily through web interfaces or web-based portals.

Colonel Ed Teague is the Chief Information Officer (CIO) and G6 at the United States Military Academy (USMA) at West Point, NY. Ed, a 1995 USMA graduate, commissioned in the U.S. Army Aviation Branch and flew the OH-58 A/C, OH-58D, and AH-1 serving in Schofield Barracks HI, Fort Drum, NY, the Republic of Korea, Arlington, VA, and Afghanistan. Ed also served in the Operation Research/Systems Analysis Branch, as an assistant professor, and as a program director in the USMA Department of Systems Engineering. Ed is currently an Academy Professor at USMA with a BS in Mechanical Engineering, MS in Operations Research from the University of Texas at Austin, and a Ph.D. in Systems Engineering from the University of Virginia.

This service access implementation paradigm allows for standardized service implementation and access for all clients, reduced developer workload, more focus on specific service entry points, and fewer service entry points that need to be monitored. Using web interfaces as a standardized access method allows standards and compliant session handling to be offloaded onto applications that implement the HTTP and HTTPS web-based protocols, such as OneDrive, SharePoint, and Office.com.

Standardizing access protocols also ensures that authentication and authorization occur through each user/service interaction and are implemented and enforced through well-defined protocol handlers. For the WREN, this has been implemented by centralizing resources access through the Microsoft Office 365 cloud-based platform. By leveraging Microsoft's authentication controls and device configuration management tools, WREN enforces correct authentication and authorization and can enforce device health controls for required resources at a per-session level. Per-session authentication and authorization (A&A) is automatically provided to all enterprise service and network architecture. Any services below the enterprise level (e.g., Academic Departments, Research teams, etc.), are not guaranteed session authentication and authorization as they exceed what the enterprise services provide.

While Office 365 provides robust session handling capabilities, the zero-trust architecture extends centralized authentication and authorization capability solely to services that understand Security Assertion Markup Language (SAML). Any services that do not support SAML must implement this level of authentication and authorization in other ways which, sometimes, do not exist for smaller or legacy applications and software packages.

ACCESS GRANTED BY DYNAMIC POLICIES

As discussed in the next section, by leveraging standards-based protocols, WREN heavily relies on HTTP and HTTPS for session management and handling. Authentication and authorization are handled through these protocols for most applications, and other checks are in place that are enforced depending on the resource being accessed. These policy checks occur through a variety of factors used to determine authorization to access a specific resource.

The first decision criterion used to access the network itself is a comply-to-connect mechanism. Devices must be known to the enterprise architecture through the mobile device management software or through the Microsoft Azure Active Directory domain and must support IEEE 802.1x network-based authentication. For devices unable to support this requirement, other options for device registration and accounting can facilitate the decision-making criteria as to whether a device can access another WREN resource. This check requires the device to be locally resident to a WREN network enclave. Implementation of a purely software defined network (SDN), as discussed in the next section, is governed by technical measures for these local network connections.

The second decision point is device health attestation. Devices must comply with several device health requirements in order to be considered healthy enough to access WREN resources. This compliance is managed through multiple means, including the mobile device management components of Office 365 and Azure Active Directory. Multiple factors are used to generate a health score. Each resource category listed above requires a minimum score. Device health is routinely monitored and devices that fall out of compliance are automatically disabled until corrected.

The third rule, which is related to the first, is geographic location. Depending on the resource type requested, geographic location could be a factor. Some resources are configured with access restricted to a certain geographic area and are hence unavailable to users outside those areas.

ALL DEVICES ARE IN THE MOST SECURE STATE PRACTICABLE

All network engineers aspire to have all connected devices in the most secure state possible, but this is an extremely limiting goal in a research or academic setting. WREN's design into multiple security types has resulted in numerous implementations to meet this requirement. The first category of resources, personally owned and completely unmanaged devices, do not require any specific security settings, because they access only public resources and lack any ability to interact with other WREN resources.

The second resource category is enterprise-owned devices which support teaching or research for a limited time but do not support network-based authentication and authorization or device health attestation. WREN's infrastructure requires no compliance model for these

devices beyond industry best practice, NIST controls, and DoD policies where applicable. While this may seem counterproductive under this model, the devices are required for a limited period and then removed from WREN.

The third resource category includes devices that support device health attestation, network compliance checks, and are integrated with the enterprise device management solution. These devices are typically mobile computing platforms (tablets and laptops) or desktops and use a common security baseline that applies a minimal number of enterprise-level controls. These devices support teaching and research and, when stringent security policies are applied, have significantly degraded performance in routine computer use (e.g., emailing), but also as a research or education computer. Functions such as code compilation, tools that are graphic-processor intensive, or need for precision response times are greatly impacted by most security policies. The security policy load is reduced on these devices, yet many enterprise policies are enforced and monitored that ensure core device health (updates, current antivirus and anti-malware, device behavior, etc.). This category contains both West Point-furnished devices and personally owned devices that require access to WREN resources. Users agree to an acceptable use and management policy agreement and allow application of WREN security policies to these devices. The ZTA implementation technology allows collection of threat indicators from both types of devices to ensure WREN data security, and to provide threat metrics and indicators to the WREN Cybersecurity enterprise.

The fourth, high-risk resource category refers to data protected by multiple regulations which, if compromised, would seriously and adversely impact the user population. Because these computing resources do not directly map to the teaching or research mission and are integral to USMA's core business, they are secured using the most stringent set of security controls.

AUTHENTICATION & AUTHORIZATION ARE DYNAMIC

One of the most difficult tasks for implementing any enterprise service delivery is providing real-time evaluation of user access to a resource. What if, post-authentication, a user's risk posture is reduced? In traditional networks, this time window provides a vector for malware or insider threat actors to access resources they may otherwise no longer be allowed to access.

WREN solves this problem through Microsoft's implementation of the Continuous Access Evaluation Protocol (CAEP),[3] which features a re-evaluation mechanism for each resource request, thus allowing resource administrator control of access to each resource on a per-request basis. This ensures that once a user's access is terminated, the time lapse between the user access revocation and access denial is limited to the time it takes to communicate between the centralized user access control and the resource provider service.

Resource access is governed by WREN's Comply to Connect (C2C) policies, and basic user role-based access (RBAC) controls. Higher-sensitivity resources, such as Privacy Act or educational record data, require the user to meet more stringent configuration polices such as coming from a West Point-issued device, within the physical network enclave of West Point, and having a user account with a low risk rating. Resources with a lower sensitivity level are accessible by users with a wider range of devices that include personally owned but Azure Active Directory-registered devices, a smaller set of security requirements, are geographically distributed, and have slightly higher risk profiles. High risk profile users have access to the smallest number of resources through the fewest number of devices. As a user's risk status rises, their ability to access resources are commensurately reduced.

ENTERPRISE COLLECTS AS MUCH NETWORK AND COMMUNICATIONS INFORMATION AS PRACTICABLE, INCORPORATING CONTINUOUS IMPROVEMENTS

WREN is designed to capture all forms of data, not only for network security but also for network optimization and performance tuning. The data capture draws from myriad sources and can be expanded to ingest nearly any type of data. WREN utilizes the capabilities of Microsoft Sentinel[4] to provide event management and automated response. Originally designed as a Security Information Event Management (SIEM)/Security Orchestration Automated Response (SOAR) platform, WREN leverages Sentinel's robust scripting capabilities as well as native integration with the Microsoft PowerBI platform to yield performance metrics both for the Microsoft Office 365 platform and for local enclave performance. This monitoring occurs through the native logging capability built into the enterprise network devices, connectors to the Sentinel platform, and automated analysis capabilities available once data are stored. Sentinel's integration capability also allows for the ingestion of external security and performance data through protocols such as TAXII and Microsoft, and other third-party threat data. This integration of external threat data along with the powerful scripting language supported within Sentinel also allows the platform to automate many response actions to event correlations which may or may not be an active threat in the network. This also allows Cyber Defenders on WREN to implement threat identification and mitigation capabilities more advanced than those existing on traditional networks.

Using data analysis, WREN's planning team can identify additional capabilities needed to expand existing and future projected capability. By monitoring network performance through Sentinel logging, Cisco DNA, and SolarWinds, network and security staff can identify service disruption due to misconfigurations, infrastructure failure, or unexpected load on key devices. Once flagged, the WREN Network Operations team corrects these service interruptions. Data trend analysis forecasts future bottlenecks or infrastructure challenges that may otherwise be unobservable. This trend analysis is critical in performance prediction and helps identify infrastructure changes, additions, or reconfigurations that can be planned as part of a long-term strategic lifecycle plan.

Collected data, while extensive, is only used to improve WREN's connectivity, throughput, service delivery, and the network's security posture. The collected data are primarily instrumentation data from network devices, performance metrics from cloud-based virtual machines, and Microsoft Office 365 performance metrics. WREN captures some user data, but it does not collect or analyze user-level data by design.

CONCLUSION

The current WREN network implementation is an imperfect model of the Zero Trust Architecture, but it can serve as a road map for higher education institutions that are designing or modifying their networks. West Point will continue to pursue a true Zero Trust Architecture for the WREN and continue to implement technologies that provide a rapid fielding capability for innovative ideas in the educational space and provide a safe, secure, and stable computing environment that leverages both security and optimization at every level found in the ZTA concept.

ACKNOWLEDGEMENTS

This research was enabled by the Department of Defense, the Department of the Army, and West Point senior leadership.

NOTES

1. M. Astani, K. Ready, and M. Tessema, "BYOD issues and strategies in organizations," *Issues In Information Systems*, 2013.
2. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST Special Publication 800-207*, 2020.
3. S. Cuff, "Azure ad security enforcement with continuous access evaluation," *URL https://bit.ly/2PtKwrB, 2020*.
4. M. Corp, "What is azure sentinel?" *URL https://docs.microsoft.com/en-us/azure/sentinel/overview,* 2019.

What Every Leader Needs Now in This Unprecedented Era of Global Competition

T. Casey Fleming

INTRODUCTION

The global pandemic forced recognition of what many already knew: the world has changed in ways that significantly alter every organization's strategic planning; few will adapt and thrive, but most will remain stagnant and perish. The world as we think we know it no longer exists. Every consequential factor, of a weakened competitive position in this new era, will cascade across our traditional landscape of responsibilities: militaries can no longer defend national borders; governments can no longer control what happens to their constituencies; and businesses are now both the primary targets and prime facilitators of global affairs.

Global trends like hybrid warfare are the new normal. They undermine trust in core institutions and the achievement of goals normally associated with military action through non-military means - and its associated tactics. For example, cyber penetration (espionage), information (cognitive) warfare, deep fake influencing, and theft of intellectual property. The new Cold War, based on highly effective hybrid warfare, has been thriving while propelling the world economy to rapidly decouple.

Corporations lacking an agile strategy and process to deal with these realities will not survive. Those that do will not only survive but thrive. The US economy is the most successful Darwinian system that has ever evolved. We can eventually win, but a majority of the companies in existence today will fail, because they came to prominence during a less competitive period of US primacy. We are back in an unstable world environment in which we, Americans, have traditionally thrived, however we must quickly adapt.

T. Casey Fleming serves as Chairman and Chief Executive Officer of BlackOps Partners Corporation, which provides strategic risk, strategy, and intelligence advice to senior leadership in many of the world's largest organizations. He regularly advises leaders of the private sector, government agencies, the military, Congress, and academia. Mr. Fleming is widely recognized as a top thought leader and keynote speaker in the areas of strategic risk, national security, cybersecurity, and unrestricted hybrid warfare. He was named Cybersecurity Professional of the Year by the Cybersecurity Excellence Awards. Previously, he led global units for IBM Corporation, Deloitte Consulting, and other management consulting and technology companies. He served as founding managing director of IBM's early Cyber division, known today as IBM Security. Mr. Fleming earned his bachelor's degree from Texas A&M University, served as guest instructor for IBM's internal MBA program, and participated in executive programs for IBM Corporation, Harvard Business School, and The Wharton School.

KEY LEADER SURVEY: POST-PANDEMIC

The year 2020 served as a critical inflection point. The entire world became simultaneously frozen, through stay-at-home orders, and reconfigured, to adapt to the new global environment underscoring the change while rendering previous assumptions and plans obsolete. Business as usual was demolished within companies and across industries. Hidden risk became revealed in the form of new financial risk, demand changes and decreases, labor shortages, and supply chain failures, to name only a few. The future is unclear, but it also presents new opportunities and new risks for those leaders who are prepared. It is a changed world, and this is the time leaders must lead in an entirely new way with a new whiteboard. During June 2021, an online and verbal survey was conducted with over 350 CEOs and government, military, and academic leaders to identify and examine the challenges top leaders are facing in this extraordinary time. This era has already been defined as unprecedented and requires an entirely new set of tools, skills, and assumptions.

NEW CRITICAL SUCCESS FACTORS EMERGED

The key leader survey revealed common critical factors that are central to future survival and success for leaders and their organizations. These include the following: (1) a continuous strategic clarity in evaluating all risk, (2) identify unseen risk to support rapid decision making, (3) agility, (4) rapid execution, 5) resilience, 6) focus on innovation.

Achieving each of these critical success factors requires an approach that is very different from any that have been used in the past. Successfully fitting these critical factors together, to harness the full power of the organization as an inherent force multiplier, will require the strategic unification of risk, strategy, the

human factor, technology, and security. The most robust method for accomplishing strategic unification and engaging the entire range of human capabilities and vulnerabilities is through a variation of business wargaming anchored in real-time intelligence.

STRATEGIC RISK REDEFINED

As 2020 unfolded, nearly every organization faced new and unprecedented risk due to the pandemic. Existing strategy and risk assumptions did not compensate for the unanticipated or hidden risk of a pandemic and, in a few cases, unseen opportunity. Further, the significant impact the pandemic would have on supply chains was completely missed. Never in recent history have companies and the global economies been so abruptly and critically impacted by unforeseen and unplanned risk.

The pandemic exposed the urgent need for a new way to identify unforeseen strategic risk across industries. It also showed how organizations need the ability to make quick decisions, pivot, and execute. Figure 1.

IMPORTANCE OF BUSINESS WARGAMES AS THE RISK PLATFORM IN THE NEW ERA

Evolving global and local risk requires a new approach to assessment and analysis that accounts for all potential contingencies. Dynamic business wargaming, an experiential process for identifying both strategic risk and unseen opportunity, has been proven by the world's most successful strategic planners in military, government, and business. Businesses require a variation on military wargaming to bring together political, technological, and environmental factors and, most importantly, people, to provide a comprehensive assessment and an action-oriented plan that cannot be achieved through any other type of analysis. A wargaming-based approach aligns every level of an organization, with shared understanding of risk and strategy, and establishes systemic agility in executing necessary change. For optimal results, the wargaming process must be tailored to each client's unique circumstances.

Almost every form of strategic analysis in common use, by business executives, exhibits three critical flaws: (1) the analyses are linear in nature rather than dynamic; (2) they are artificially objective, creating a false sense of certainty; and (3) they are collaborative in their incentives, which prevents the rigorous critical thinking that would yield the desired objective. These shortfalls, collectively, cause both important risks and potential opportunities to be missed. For centuries, wargaming has served military leadership reliably as a way to avoid these pitfalls by allowing decision makers to experience and assess potential futures at very low cost. This approach can greatly reduce aggregate risk in the increasingly complex, dynamic, and competitive environment accentuated by the pandemic.

What makes wargaming different is the handling of the inherently irrational element of human decision-making. Even economists increasingly admit human beings are not always rational actors. Yet much of business analysis tacitly assumes they are, and proceeds with "objective" assessments that provide a false sense of accuracy and certainty. Wargames draw out the emotion and inherent irrationality that accompany human beings making decisions under stress and with imperfect information. They also offer incentives for an exploration of the full range of challenges that competitors or changes in the business environment might pose—no matter how inconvenient or improbable they might be. You must face competitors and evolving circumstances as they are or may turn out to be, not as you wish them to be.

In addition to developing and testing strategy, wargames offer several collateral benefits. They train participants in critical thinking; help both participants and their management evaluate their decision making under stress; draw out input from those at junior levels of the organization who might not normally have the mechanism, incentive, or permission to contribute; show whether risk or opportunity is greater than expected due to scattered distribution across several parts of the organization and/or its supply chain; draw out assumptions and challenges through group-think that might otherwise remain hidden; and help align teams toward a shared understanding and shared course of action.

Business wargames are a pivotal tool for every organization seeking to reduce risk or identify opportunities ahead of their competition. Effective wargames can range from a few hours, for senior leadership, to several days, for senior and mid-level staff. The length and scope depend on the complexity of the situation(s) being assessed and the level of detail desired.

REAL-TIME INTELLIGENCE

Economic espionage and the case for corporate counterintelligence in today's hyper-competitive global environment, static wargames and risk modeling are ineffective without a foundation in real-time counterintelligence. Nation-states and corporations have historically utilized business wargaming to gain strategic advantage against US and western enterprises. Wargame scenarios and outputs must be continuously measured against known threats, risks, adversarial strategies and actions for the most accurate results.

TECHNOLOGY AND SECURITY

To remain competitive, companies are required to focus on a pipeline full of innovation to maintain leadership in both global and local markets. While innovation is important, securing intellectual property must be paramount. Ongoing technology campaigns—for example, digital transformation, hybrid cloud, and artificial intelligence—must treat security as an integral part of development.

LEVERAGING THE HUMAN FACTOR

The human factor is the force multiplier in every organization. Over the years, efforts have fallen drastically short in harnessing and efficiently leveraging the collective power and security of employees, contractors, and suppliers. Survival and success require a culture in how we view our role in the new era of global competition. This can be accomplished by business wargames.

SUMMARY

It has been said that within every crisis, there is also opportunity. This is the time for leaders to engage this unprecedented era of global competition by leading in an entirely new way—through the unification of strategic risk, strategy, the human factor, technology, and security—facilitated through the power of business wargaming. Leaders and their companies must achieve new critical factors of: clarity in strategic risk, identifying unseen risk and opportunities, agility, resilience, rapid decision making, and the ability to prioritize quickly and pivot for execution.

Experiential process for identifying both strategic risk and unseen opportunity has been proven over 150 years by the world's most successful strategic planners in military, government, and business. We use a variation on military wargaming to bring together political, technological, environmental and *most importantly* human factors to provide a comprehensive assessment and an action-oriented plan that cannot be achieved through any other type of analysis. This approach aligns every level of an organization in shared understanding and provides elevated agility in executing necessary change. The process is bespoke tailored to each client's unique circumstances.

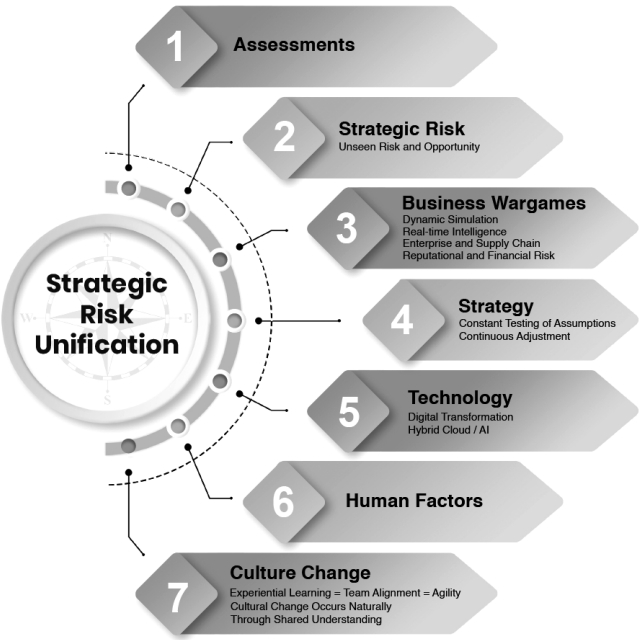


Figure 1. Process for Identifying Strategic Risk and Unseen Opportunity

Experiential Business Wargaming: Required to Survive and Succeed in this Unprecedented Era of Global Competition

Practical Cyber Risk Management for Tactical Commanders

Colonel Ron Iammartino

ABSTRACT

Risk management in today's complex threat environment necessitates decision rules that integrate cyber risk control into the overall mission risk profile. This article outlines cyber risk management decision rules that are based on lessons learned from the Expeditionary Signal Battalion-Enhanced (ESB-E) prototype, which adapted Special Operations Forces (SOF) and commercial-off-the-shelf (COTS) capabilities by applying a rapid fielding and feedback approaches within the scope of the Army Futures Command. Focus areas include the use of diverse COTS systems and satellite communications providers to mitigate risk, controlled system maintenance processes, capitalizing on behavioral bias in cybersecurity, integrating enterprise services, and keeping pace with technological innovation trends. Lessons learned are intended to give tactical commanders practical cyber risk management options within the overall scope of mission risk management.

Risk management in today's complex threat environment necessitates decision rules that integrate cyber risk control into the overall mission risk profile. A decision rule is a statistical term that operationalizes principles through pre-determined decision criteria or algorithms for faster, authoritative risk management decision-making.[1] Network jamming, disruption, and penetration threats can change at a pace that outstrips enterprise-level resources available in a contested or congested electromagnetic (EM) environment.[2] Predetermined decision rules that provide practical risk management options appear to be particularly important for tactical units, since these units deploy on short notice to austere and rapidly changing environments where network management controls are limited. As demonstrated during two sensitive

Colonel Ron Iammartino is a U.S. Army Signal Officer. He is currently the Army War College Fellow at Princeton University and most recently served as the Commander of the 50th Signal Battalion at Fort Bragg, NC. He previously served as an action officer on the Joint Chiefs of Staff and the Department of Army Staff in Washington, DC. He holds a Ph.D. in Systems Engineering from the George Washington University, an MA in Quantitative Methods from Columbia University, and an MBA in Finance from Monmouth University. He is a 2003 graduate of the U.S. Military Academy. His prior published work focuses on agent-based and statistical modeling..

Immediate Response Force (IRF) missions in 2019-20, division and brigade commanders now have access to decision rules and technologies that can more quickly shape communications systems capabilities within an operational environment without strict dependence on the enterprise to mitigate network risk.

Accordingly, the Army has undertaken a series of coordinated network modernization efforts intended to experiment with the adaptation of emerging commercial technology to improve tactical network resilience.[3] One of these efforts is called the Expeditionary Signal Battalion-Enhanced (ESB-E) prototype. The prototype calls for tactical communications assets that are faster, lighter, and easier to employ. These assets are largely modeled after Special Operations Forces (SOF) capabilities that had previously been limited to lower-scale development.[4] Whereas past conventional capabilities were deployed with a one-size-fits-all solution exposed to shared risks across the enterprise, the ESB-E provides supported commanders with far greater options for managing cyber risk across a more diverse set of command and control (C2) asset alternatives. This paper outlines decision rules that are based on lessons learned from the ESB-E prototype intended to give tactical commanders practical cyber risk management options within the overall scope of mission risk management.[5] These decision rules are related to employing multiple information technology (IT) vendor solutions, a range of satellite and cellular service providers, centralized maintenance processes and validation, the use of enterprise services for redundancy, a bias toward sharing with coalition mission partners, and leveraging commercial technological innovation trends.

The first decision-rule is to employ several different vendor solutions to mitigate hardware security risk as a means to ensure capability reliability. The ESB-E is comprised of IT solutions from a range of different vendors and service providers. This approach helps

manage risk exposure in that the risk to one system or communications kit is not evenly distributed across the full capability set as in past technology upgrades. One ESB-E component, for instance, may be particularly vulnerable to a software bug, supply chain risk, or embedded hardware faults attributable to a threat originating in the Pacific area of responsibility, while another is more vulnerable to a threat originating from a non-state actor in Europe.[6] The differences within the ESB-E capability set significantly reduces the risk that a single hardware or manufacturing vulnerability can result in a catastrophic outage.

A second decision rule is to test and enable multiple military satellite, commercial satellite, and cellular transmission paths as condition for deployment. One might think of each respective satellite and cellular transmission path as representing a distinguishable and mutually exclusive route for accessing military networks, which is comparable to having multiple cellular providers and cable Internet packages. The idea is to get into the network securely any way you can.[7] The ESB-E has far greater flexibility for employing communications assets across SATCOM bands and commercial infrastructure, such that units can more easily adapt support in a degraded or contested electromagnetic spectrum communications environment.[8] Probabilistically, it is harder for an adversary to jam or deny network access to a user that can access defense networks through more than one means simultaneously.[9] This approach is analogous to the Army targeting guidelines in that the ESB-E model makes it more difficult to isolate or fix on a target that has an ambiguous or wide area attack surface.[10]

This emphasis on a probabilistic approach to mission management and risk is key to these first two decision rules. Even commanders without access to ESB-E resources can benefit from this construct in terms of understanding where their unit may have concentrated risks. The Primary, Alternate, Contingency, and Emergency (PACE) approach to communications risk management must be broken down into dimensions that allow commanders to understand where there is more than a single point of failure in each network layer. Predetermined decision rules that have already incorporated the probabilities of these risks and appropriate mitigation strategies are critical to the continuity of communications support to operation in a congested environment. In one recent example, a brigade-level IRF commander, who did not have access to ESB-E resources was able to immediately transition to a commercial satellite while waiting for repair components to fix failed organic government satellite assets. The commander had preplanned this decision through pre-mission training that included a pilot program commercial satellite system.

The third decision rule mandates that all systems go through a higher headquarters-controlled pre-mission and post-mission maintenance reset process as a condition for unit deployment. In line with the 2015 Defense Cybersecurity Culture and Compliance Initiative (DC3I), the ESB-E centralized maintenance and reset process helps to reduce common human errors through external validation and standardization prior to active employment. It also gives commanders better visibility on asset readiness. The centralized maintenance and reset

process applies the DC3I principles of dual verification, specific reset role assignments, and external validation for ensuring predictable readiness standards for all assets.[11] The process calls for all ESB-E assets to be inspected and validated in deliberate phases by communications-electronics (C&E) hardware and network operations (NETOPS) software sections in order to verify that all systems have functional hardware, the latest software version, and cybersecurity patches. It further includes an external certification through the Brigade NETOPS tactical hub to help identify and reduce errors during reset. In addition, the approach centralizes asset visibility on high-failure rate components, factory recalls, and other deficiency trends to facilitate knowledge transfer on risk.[12]

More generally, the centralized maintenance process reinforces better alignment with higher headquarters, together with closer cross-functional team integration between operations and maintenance so fewer risks can go unnoticed. This is akin to the cultural norms for dual verifications and external system maintenance checks long ago established by the nuclear Navy, which, until recently, have been hard to replicate on sometimes-dormant tactical network systems sitting in a large motor pool.[13]

A fourth decision rule is to select enterprise services as a back-up to any organic voice or video services for use during deployment. In the past, tactical units were limited to organic systems and devices for capabilities such as phone, email, or video teleconference during a deployment or exercise. In contrast, the ESB-E can much more easily use enterprise home-station capabilities due to its more advanced and lighter Internet protocol (IP) based routing systems. This has the potential to help with eliminating common human errors in cybersecurity, while also ensuring network and risk convergence across the enterprise. Risk is better balanced by the common standards, less proprietary complexity, authoritative identity management features, and increased service delivery mixes characteristic of enterprise services, such as enterprise email or Defense Information System Agency (DISA) global video services (GVS). At ROVING SANDS 2019, for instance, ESB-E teams were able to employ enterprise services seamlessly for secure voice communications when a network access denial prevented call-routing using organic call manager assets.[14] Even more, tactical units can more easily keep pace with changing threat vulnerabilities through reliance on enterprise-level software updates, rather than local replacement of vendor-specific systems or software.[15]

A fifth decision-rule is to default to coalition partner information sharing when partners achieve predetermined COTS system cybersecurity standards. A large body of behavioral science research suggests that decision-makers are inherently biased toward risk aversion in that they tend to avoid losses more than taking prudent risks to improve information-sharing.[16] This tendency runs counter to the DOD and CJCS 2017 objective to establish a bias toward sharing with allies and mission partners.[17] ESB-E, however, seems to help to reinforce the objective to take reasonable risks – and improve network interoperability through COTS, its open architecture that provides allies and partners with standards-based alternatives for

interoperability instead of the acquisition of a single, closed proprietary hardware requirement. These considerations, combined with the previously outlined improvements to enterprise network visibility and ESB-E maintenance processes, encourages better cybersecurity readiness transparency among allies, thereby stimulating more operationally effective network management policy decisions that bias toward safer information sharing.[18]

Further, commanders can set a decision rule to use the ESB-E rapid prototype approach to deliberately capitalize on commercial market trends in technological innovation. It has become much tougher for a single vendor or product to maintain market dominance. Open-source innovation makes breakthroughs in capabilities or cybersecurity more accessible at lower cost.[19] The top technology firms today are competing for much smaller incremental improvements than the major advances that were achieved by technology firms like Facebook and Google in the early 2000s.[20] These trends make it far easier for ESB-E rapid prototyping of new technology to inform upgrade decisions, thereby adapting cybersecurity readiness more quickly.

This article emphasizes the importance of commander engagement to expand options and access to network resources, systems, and new technologies to manage risk. It prioritizes increasing access and availability for effective communications over cybersecurity defense limitations. Past work has shown that rigorously stress-testing new equipment, particularly when it is completed on live networks in partnership with tactical units, helps to ensure that security measures do not overly burden commanders with enterprise risk controls or change management inconsistencies.[21] Yet, commanders must be aware of the tradeoffs in potential exposure to unknown cyber risks associated with new or open-source technologies, such as zero-day vulnerabilities. The importance of strong controls, such as the aforementioned centralized maintenance process, end-point security, user training and discipline, multi-factor authentication, and network monitoring should not be understated.

In sum, there are six key conclusions from this article that can be practically applied to strengthen tactical cybersecurity risk management. The first two overlap. First, units should take advantage of the better technology and smaller form-factors of emerging capability sets like ESB-E and by having multiple solutions to solve a single IT or signal problem. Having options helps mitigate cyber risk associated with hardware vulnerabilities or enterprise inefficiencies that may not be resolved in a timely manner for a single system. Second, units should ensure the employment of multiple SATCOM bands and cellular service providers. It should not be assumed that these assets are readily available through unit training or enterprise-level resourcing without command emphasis. Third, commanders can leverage a controlled maintenance reset process to deliver an accurate picture of cybersecurity and system readiness. Fourth, commanders should apply COTS cybersecurity standards and behavioral science insights to reinforce a bias toward information sharing with coalition partners. Fifth, tactical commanders should emphasize the integration of enterprise services as part of the tactical communications plan to provide redundancy and network security reinforcement.

Finally, technological innovation trends suggest that rapid prototyping is an appropriate means to test and adopt new technologies, since smaller incremental technology improvements and open source software are characteristic of the emerging IT market environment. Rapid prototyping, as described through the ESB-E use prototype can help Army tactical units keep pace with changing cyber threats.

ESB-E is one of many ongoing initiatives contributing to better cybersecurity risk management across the Army. Future efforts should incorporate more sophisticated artificial intelligence and quantum computing risks. Cyber risk will also soon be impacted by the advance of 5G, Mid-Earth Orbit and Low Earth Orbit satellites.[22] Decision rules must consequently evolve as practical tools for tactical commanders.[23]

NOTES

1. Carl Hauser, Yeow Meng Thum, Wei He, and Lingling Ma, "Using a Model of Analysts' Judgments to Augment an Item Calibration Process" *Educational and Psychological Measurement* 75, no. 5 (October 1, 2015), 826-49, https://search-ebsco-host-com.proxy1.ncu.edu/login.aspx?direct=true&db=eric&AN=EJ1073524&site=eds-live.
2. Ray Dalio, "Principles: life and work." First Simon & Schuster hardcover edition. New York: Simon and Schuster, 510-523.
2. Joseph Lacdan, "G6: Greater Integration across unified network will strengthen force," *Army News Service* (October 30, 2020), https://www.army.mil/article/240404/g_6_greater_integration_across_unified_network_will_strengthen_force, accessed November 3, 2020.
4. Amy Walker, "Army Pilots New Signal Battalion for Scalable Expeditionary Comms Support," *PM Tactical Network/PEO C3T Public Affairs,* October 11, 2018, https://www.army.mil/article/212220/army_pilots_new_signal_battalion_for_scalable_expeditionary_comms_support, accessed September 1, 2020.
5. Ron Iammartino, "ESB-E Cyber Risk," White Paper, January 2020, Unpublished Manuscript.
6. Ruby B. Lee, "Security Basics for Computer Architects," Morgan & Claypool, 2013, 1-10.
7. This concept is based on discussion and input from the 50th ESB-E Network Operations Section in January 2020.
8. Ibid.
9. Iammartino, "ESB-E Cyber Risk."
10. Army Techniques Publication 3-60: 2015.
11. U.S. Department of Defense, "Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)." October 2015, 1-12.
12. Ron Iammartino & Christopher O'Connor, "Army Networks at a Crossroads," *ARMY Magazine,* August 2019, 1-3.
13. Ibid.
14. Iammartino & O'Connor, "Army Networks at a Crossroads." ARMY Magazine, 3-5.
15. Ron Iammartino, Todd Doherty, & John Fossaceca, "Transforming DoD Information Technology Networks through Coalition Partner Trust," *Small Wars Journal,* 12 (1), December 30, 2018.
16. Amos Tversky & Daniel Kahneman, "Judgment under uncertainty: Heuristics and biases," *Science,* (1974), 185(4157), 1124-1131.
17. General Joseph F. Dunford, "Allies and Partners Are Our Strategic Center of Gravity," *Joint Force Quarterly* 4, no. 87 (2017): 5.
18. Ron Iammartino, Todd Doherty, & John Fossaceca, "Transforming DoD Information Technology Networks through Coalition Partner Trust." *Small Wars Journal,* 3-5.
19. "Tech firms are suddenly the corporate world's biggest investors." *The Economist*, July 28, 2018, https://www.economist.com/business/2018/07/28/tech-firms-are-suddenly-the-corporate-worlds-biggest-investors, accessed November 3, 2020.
20. "Silicon Valley's giants look more entrenched than ever before" *The Economist.* August 10, 2019. https://www.economist.com/graphic-detail/2019/08/10/silicon-valleys-giants-look-more-entrenched-than-ever-before, accessed November 3, 2020.
21. Ron Iammartino, "Army Networks at a Crossroads."
22. Ron Iammartino, "ESB-E Cyber Risk."
23. Author Note: Sections and ideas throughout this article have, in part, been derived from a series of experiences and white papers written during my time in command of 50th ESB-E, Fort Bragg, NC. Many of the ideas and concepts are based on the lessons learned, input, and mission employment of capabilities by 50th ESB-E soldiers, non-commissioned officers, and officers. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

Information Advantage Activities:

A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations

Lieutenant Colonel Robert J. Ross, Ph.D.

INTRODUCTION

The Multi-Domain Operations (MDO) doctrinal framework is the driving mechanism for transforming the U.S. Army into a dominant information-age military force. To address the informational power aspects associated with MDO, the U.S. Army's Training and Doctrine Command (TRADOC), in partnership with the Cyber Center of Excellence (CCoE), developed the Information Advantage (IA) and Decision Dominance (DD) doctrinal framework. Within this framework, "commanders seek to achieve DD, a desired state in which a commander can sense, understand, decide, act, and assess faster and more effectively than an adversary by gaining and maintaining positions of relative advantage, including IA."[1] IA is "a condition when a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision-making using all military capabilities through the conduct of Information Advantage Activities (IAA)."[2] Lastly, IAA is defined as "the employment of capabilities to enable decision-making, protect friendly information, inform and educate domestic audiences, inform and influence international audiences, and conduct information warfare."[3]

The exponential growth in powerful computer network technologies and its effects on human cognition are radically changing the character of 21st century warfare. The unceasing pace in the growth of Internet of Things (IoT) devices has created ubiquitous human access to voluminous amounts of information. This access, coupled with the individual's ability to influence global audiences from these devices, is creating radical social and political change across the world, including the character of warfare. The technological and cognitive effects stemming from using these devices have been demonstrated within conflicts waged thus far in the century. These conflicts have demonstrated that the means for waging war depends more and more on artificial intelligence, machine learning, computer networks, and autonomous/semi-autonomous vehicles. The U.S. Army is at a point

Lieutenant Colonel Robert J. Ross is the Strategic Initiatives Group Chief for the Commanding General of U.S. Army Cyber Command, Fort Gordon, GA. Lieutenant Colonel Ross advises the ARCYBER Commanding General on cybersecurity, information-age conflict, and information warfare strategy initiatives. Lieutenant Colonel Ross is a former assistant professor in the Electrical Engineering and Computer Science Department at United States Military Academy at West Point, NY. As an assistant professor, Lieutenant Colonel Ross taught primarily information technology courses and course directed the Academy's information warfare course. He is a former Chief Research Scientist for the Army Cyber Institute, where he served as the Information Warfare Team Lead. Lieutenant Colonel Ross has a B.S. in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Lieutenant Colonel Ross is a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare, 21st century conflict, and financial technology.

in which all six of its warfighting functions (Movement and Maneuver, Intelligence, Fires, Protection, Sustainment, and Mission Command) will be totally dependent upon the Army's portion of the Department of Defense Information Network (DoDIN) to effectively conduct MDO by 2028.

The changing character of warfare in the 21st century should serve as a catalyst for the U.S. Army to reexamine its contextual view of information, how is used to describe capabilities, and how operational art is applied within the IA and DD doctrinal framework. The word "information" is used broadly throughout Army doctrine and literature. There are 259 instances of "information" used within Field Manual 1-02.1, which defines information as "in the context of decision-making, data that has been organized and processed to provide context for further analysis."[4] Before the publication of Field Manual 1-02.1, there was no definition for the word "information" within any U.S. Army doctrine. However, this semiotic definition begs further explanation, particularly regarding the role information plays within the human dimensions of operational environments. Members of the Army community have many different understandings of how "information" is used within mixed professional specialties on Army staffs. The many differing definitions of the word "information" are dependent upon the context of its use. Unfortunately, dependent upon branch or military occupational specialty (MOS), interpretations of the context will lead to misunderstanding. These differing perspectives or contexts used to understand the meaning of "information" affect its usage, particularly as it applies to capabilities and operations. This article aims to raise the philosophical and contextual question, "what is information?" within the context for Army operations then examine its application across the range of capabilities and current operational art.

Information is inherent in every capability at an Army commander's disposal. The combination of

organization, strategy, and integrated technologies defines a capability regardless of context. Understanding this informational principle about a capability removes the confusion, misunderstandings, murkiness, and ambiguities associated with categorizing it as "information-related." Every capability is "information-related" and popular definitions for "information" in the academic and information science literature support this assertion. Therefore, the Army should eliminate the term, "information-related capability," during the development of future IA capabilities. A second proposition would be to maintain a more traditional view of capabilities with the caveat that a capability is more than a material resource or technology. It is a system comprised of organization, strategy, and integrated technology. Operational art is defined in Army doctrine as a "cognitive" process that involves "skill, experience, creativity, and judgement," therefore, contemporary operational art requires a holistic approach unrestrained from the ambiguous categorizations associated with the term, "information," or its use as an adjective for capabilities. Such categorizations are constraining and get in the way of the efficient deployment of capabilities in 21st century operating environments. Therefore, an amenable model is proposed later in the paper as a base of knowledge for discussions about future Army organization and the role of information within the commander's operational art at all levels of Great Power Competition.

WHAT IS INFORMATION?

Meaning and context are the two biggest challenges for the Army's use of the word "information," particularly when it is used to categorize an "information-related capability." Information is too abstract and omnipresent to be treated as an entity of its own within the operational environment. The cyberspace operations, electromagnetic warfare, and signal community often view information within the context of Shannon and Weaver's telecommunications research. They define "information" within the context of mechanistic or engineering perspectives.[5] These communities view information through the lens of digitization, radiated frequency, or optical signals. Conversely, PSYOP, public affairs, and information operations professionals view information from a perspective more akin to Howell's definition in which information is defined as "not only facts and figures, but all the relationships, vague ideas, hunches, feelings, in fact, everything people have stored inside them or have picked up from the outside world." [6]

This same notion holds true in the military intelligence community, which views cyber intelligence information using both mechanical and cognitive lenses. Intelligence professionals working in the cyber community view social media, commercial cyber vulnerabilities, or advanced persistent threat (APT) information in all forms, often from proprietary sources, in a context that does not typically integrate well with traditional forms of military intelligence. People can have various understandings of what information is within a particular Army operation, therefore, "information" and the context in which it is being used cannot have a common understanding or definition. This is particularly true as it pertains to the varying and voluminous amounts of information used for decision-making and the use of capabilities.

Information should be novel and inform its human consumers. However, larger philosophical and contextual questions need to be answered before a consensus can be reached on the use of the term within Army operations, including its use as a description for capabilities. Does data received from sensors which are a part of an automated system, then analyzed, and used in automated decision making constitute "information?" What about digitized, electrical representations of information residing on computers or being transported across a network? Some would argue that artificial intelligence and machine learning counter the proposed philosophy that information is purely a human process.

However, for argument, the Army, as an organization, is currently a human information processing entity.[7] It exists to acquire and process information used for human—not artificial—decision-making. It also exists within a military context to disrupt, degrade, deny, destroy, or manipulate adversarial organizations' information acquisition and processing capabilities while doing the same concerning their cognitive will to fight. Taking a practical view of information will remove much of the ambiguity, confusion, murkiness, and misunderstandings that terms like "information-related capabilities" convey. All capabilities should be treated as information-related capabilities, which would summarily eliminate categorizing labels that describe capabilities as either information-related or kinetic. Distinctions between capabilities, particularly when commanders are integrating information warfare capabilities (cyberspace, electromagnetic warfare, and information operations) into combined arms operations (infantry, armor, and artillery) during conflict hampers the application of their operational art.

CAPABILITIES VERSUS INFORMATION RELATED CAPABILITIES

> "Everything we say and do, and everything we fail to say and do, will have an impact in other lands. It will affect the minds and the wills of men and women there."
>
> *- Presidential candidate Dwight D. Eisenhower, campaign speech, 1952*

It must be inculcated into the Army's culture that all capabilities at commanders' disposal are information related. Whether firing suppressive fires through artillery or amplifying narrative supporting Army operations across social media to a targeted audience, it makes no difference, "information" affecting human cognition is still being conveyed during the application of a commanders' operational art. All actions, communications, and even the identity the Army conveys to populations for whom they are engaged, conveys information, because, intentionally or unintentionally, the Army's presence influences the behaviors of these societies simply as an outcome of the capability's the commander is leveraging during operations. The United Kingdom's (UK) Ministry of Defence uses a similar concept conveyed in their Defence Strategic Communication Doctrine Note. This document defines operations in the information environment as "advancing national interests by using Defence as a means of communication to influence the attitudes, beliefs, and behaviours of audiences."[8] Most importantly, this document does not view information as a separate and distinct entity from

the diplomatic, military, and economic instruments of national power. The Joint Note defines information as the integrating function, the glue, binding the instruments of national power together.[9] A definition and philosophical understanding that should be adopted within the context of the IA doctrinal framework and commanders' operational art.

Figure 1. Information's relationship with the instruments of National Power.
Diagram adapted from the Joint Doctrine Note 2/19.

Information and the contemporary information dimension of operational environments pose significant challenges for the Army of the future. The exponential growth of technological innovation coupled with a global society consuming information from the vast and ad-hoc socio-technical networks being formed are creating complex operational environments. These technologies cause the planning and deployment of capabilities to become more complicated by attempting to distinguish information-related capabilities from all other capabilities at a commander's disposal. This is particularly true as nearly every capability within the auspices of the Army's six warfighting functions is dependent upon the vital data flows streaming across the Department of Defense Information Network – Army (DoDIN-A). This is a condition that will only become more pervasive as the growth and reliance on powerful technologies grows exponentially in the foreseeable future. Every Army weapon, command and control, signals intelligence, and sustainment system is dependent on a functional and secure DoDIN-A to successfully train, deploy, sustain, and support winning the joint fight in contemporary operating environments. If commanders are going to successfully adapt to tomorrow's technologically driven operational environments, the focus should be on viewing all capabilities as conveying information and considering the network as part of the combined arms fight within the application of operational art.

Like our British Allies have done with their national defense strategy, the U.S. Army should create capabilities (organizations, strategies, and integrated technologies) with the view that information is not a separate or distinct framework, such as maneuver versus support. It exists within the integrated components of all warfighting functions. Instead of distinguishing information-related capabilities from all other capabilities, we should inculcate a culture that views the use of all the commander's capabilities for the purposes of information advantage activities in competition, crisis, and conflict. An example would be firing an artilery round for the purposes of getting enemy counter-fire radar to radiate, then using electromagnetic warfare capabilities to detect the radar's location, then jam its location, and finally, an air asset to subsequently destroy the radar. In this example, the commander uses a range of unique capabilities to conduct information advantage activities that first disrupts then destroys an adversary's abilities to conduct signals collection activities.

The U.S. Army's concepts and strategies of the future need to be based on the commander's operational art, defined as "the principles of joint operations to envision how to establish conditions that accomplish their missions and achieve assigned objectives" using the combination of all capabilities at their disposal.[10] The future operational art will require that commanders apply the range of their capabilities as information advantage activities during periods of competition, crisis, and conflict. War is a clash of human will and the will is a cognitive function; therefore, all actions—physical, informational, violent, non-violent, however they are categorized—are intended to achieve cognitive effects. The commander's goal should be to destroy the adversary's will to fight without fighting.[11] We would be best served to eliminate categories that ultimately impede the commanders' operational art.

CONSIDERATIONS

Before proposing an organizational view for the future information-advantaged force, the U.S. Army needs to consider the following:

a. Free market innovation, research, and development have created exponential growth in socio-technical networks through the availability of inexpensive, commercial-off-the-shelf (COTS) technologies that provide state and non-state actors' information parity with the U.S. in most operational environments.[12]

b. The current military acquisition processes are intended for success in the 20th century, the era of industrialization, not the information-age. The rapid availability of cheap COTS equipment renders most of the Army's information technology equipment and battlefield operating systems (BOS) obsolete long before they are fielded.

c. Information advantage activities faced by the Army should be dependent on strategy, not solely on information technology.[13]

These considerations serve as a framework for describing and explaining the role of information advantage activities within a commander's operational art.

OPERATIONAL ART AND INFORMATION ADVANTAGE ACTIVITIES

Information activities are persistent and not bound by the traditional phases of operations; they persist across all phases of military operations for which commanders are responsible (Competition → Conflict → Return-to-competition).[14] Since all capabilities at a commander's disposal are intended to deny, delay, disrupt, destroy, or manipulate information, information advantage activities need to be raised to a continuous level of consciousness among commanders and their staffs during the application of operational art. Cultural change concerning information and its application within operational art must be adopted throughout the Army's professional military education (PME) system for all levels of Army leadership.

Information advantage activities are continuous across all phases of military operations whose outcomes are intended to be either coercive or non-coercive. They are dependent on a powerful Army network that serves as a global projection platform capable of transporting, storing, and processing voluminous amounts of holistic and real-time information. The goals for these activities should be integrated, coordinated, and synchronized across the strategic, operational, and tactical levels and focused on achieving US strategic aims during Multi-Domain Operations. The goal of information advantage activities is to enable commanders to achieve decision dominance and ultimately break an adversary's will to fight before reaching armed conflict.[15] The challenge will be inculcating a culture that adopts some variation of the proposed information advantage activities' definition and is willing to apply it to the application of operational art.

A good analogy for this conceptual view could be defined as looking at the operational environment from the perspectives of quantum (multiple) states versus binary (two) states (Johnson, 2019).[16] In the quantum view, the human, physical, and information dimensions of an operational environment are integrated, continuous, and interconnected. Events and activities are connected and impact all three dimensions of the operational environment simultaneously, rapidly, and unpredictably across both time and space. The physical and human dimensions, independent of the information dimension, exist in a binary-like state in which activities have probabilistically predictable conclusions that are observable and measurable in ways that commanders can understand and effectively respond. Subsequently, effects in the information dimension, at the level of human cognition, are persistent and reside in an infinite state, the effects of which are not always observable, measurable, or predictable. The proposed information advantage activities concept could serve as a mechanism for bridging the divide in how commanders view the operational environment as a gestalt comprised of the physical, human, and information dimensions. It must be emphasized that the information advantage doctrinal framework is designed to add to a commander's operational art, not take away current applications of the form. The U.S. Army's ability to kinetically overmatch our adversaries and break their will to fight during periods of armed conflict must be maintained.

PROPOSED CONCEPTUAL INFORMATION ACTIVITIES MODEL

The following proposed model provides a view that maintains the Army's current warfighting function (WfF) posture.[17] Note the model illustrated in figure 2 does not add a separate and distinct information warfare WfF. Rather it is intended to change the way commanders view all the capabilities at their disposal and the role of persistent information advantage activities across all phases of military operations.

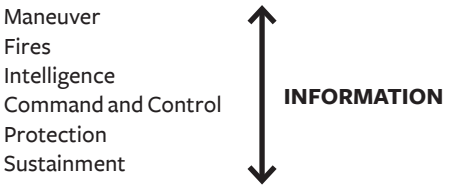


Figure 2. Information's relationship with the U.S. Army's WfF.

Figure 2 above illustrates a view that reflects information as an integrating element of all WfFs as adapted from the UK's Joint Doctrine Note 2/19. This figure reflects the role of information as pervasive across all WfF and likewise across the range of capabilities available to commanders. Capabilities are used to enact the commander's operational art, and all capabilities are considered information related.

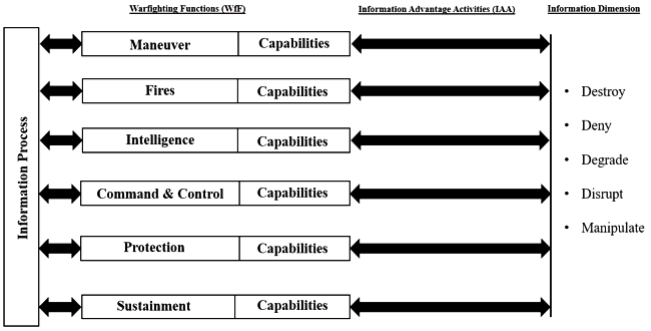


Figure 3 The role information advantage activities within the commander's operational art.

Figure 3 above illustrates the Army organization as an information processing entity. It illustrates the information processing relationship between the Army's WfFs that are integrated, synchronized, and coordinated. It also illustrates how capabilities executed by the WfFs are intended to analyze or react to information advantage activities within the operational environment.[18] The figure also presents a typology for intended information advantage activity outcomes. Information advantage activities are intended to acquire information, disrupt information, engage with populations (influence/inform), or destroy sources of adversarial information activities. Information advantage activities are persistent and constant, while military operations across competition, crisis, and conflict are dynamic. The model is intended to integrate the range of kinetic, non-kinetic, coercive, and non-coercive capabilities at a commander's disposal in a way that eliminates the confusion, ambiguity, murkiness, and tribalism that would be created by defining information as a new warfighting function (WfF).

CONCLUSIONS

This article presented information advantage activities as core components of the Army's new Information Advantage and Decision Dominance doctrinal framework. It also proposed

a definition and model for the deployment of capabilities at the commander's disposal during their application of operational art. The proposed definition and model are intended to remove the confusion, misunderstandings, murkiness, and ambiguities created by categorizing capabilities as "information-related." It also explains the causes for confusion between the different warfighting functions when the term "information" is used based on different understandings, meanings, and contexts for the terms of use between these groups. A couple of definitions of information from the academic literature support this assertion. As a result, this article proposes eliminating the term "information-related capabilities" because all capabilities are information-related. Distinguishing between what is a capability and what is an information-related capability creates a far more complicated view for how commanders see themselves, see the adversary, understand, decide, act, and continually assess during the application of operational art within contemporary operational environments. These complicated views cause the events involving information for decision-making to become blurred and the commander's actions involving capabilities to be unsupportive of one another instead of coordinated. The UK's Ministry of Defence's Joint Doctrine Note 2/19 Defence Strategic Communication: An Approach to Formulating and Executing Strategy was used to support this functional view.

Finally, a model is proposed that does not view the physical, human, and information dimensions as separate entities. Instead, it provides a view of the operational environment as a gestalt in which the physical, human, and information dimensions are fully integrated parts. Again, this model is supported through example found in the UK's Ministry of Defence's Strategic Communication: an Approach to Formulating and Executing Strategy, Joint Doctrine Note 2/19, in which information is viewed not as a separate instrument of national power, but the glue that binds diplomacy, military, and economic power together. [19] The same view should be adopted within the Army's culture in which information is not viewed as a separate or distinct component within the operational environment, but the glue that flows through and binds together every capability enabling operations. In closing, the model presented as a concept in this paper integrates information advantage activities in a way that adds to our current model for the application of operational art and does not take away from it. Adopting these proposed views into Army culture surrounding use of the term "information" and the future application of operational art will only reinforce IA and DD as a doctrinal framework that will effectively support future multi-domain operations (MDO).

ACKNOWLEDGEMENTS

The author would like to thank Lieutenant General Stephen G. Fogarty (Commanding General, U.S. Army Cyber Command) and Mr. Bryan Sparling (U.S. Army Cyber Command's Information Warfare Transformation Advisor) for the invaluable insights they provided to this article.

NOTES

1. U.S. Army Training and Doctrine Command, 2021, *Information Advantage and Decision Dominance version 15*, unpublished Whitepaper, Fort Gordon, GA.
2. Ibid.
3. Ibid.
4. U.S. Department of the Army, 2021, *Field Manual 1-02.1 Operational Terms,* Washington, DC.
5. C. Shannon and W. Weaver, *The mathematical, theory of communication* (Champaign, IL: University of Illinois Press, 1963).
6. W.S. Howell, *The empathic communicator* (Belmont, CA: Wadsworth, 1982).
7. J.R. Galbraith, *Organization Design* (Boston: Addison Wesley, 1977).
8. U.K. Ministry of Defence, 2019, *Joint Doctrine Note 2/19 Defence Strategic Communication: an Approach to Formulating and Executing Strategy*, Shrivenham, Swindon, Wiltshire, 4-17.
9. Ibid.
10. U.S. Department of the Army, 2017, *Field Manual 3-0 Operations.* Washington, DC.
11. S. Tzu, 1971, *The art of war* (Vol. 361). Oxford University Press, USA.
12. B.D. Johnson, D. Alida, J. Brown, and R.J. Ross 2020, *Information Warfare and the Future of Conflict,* Arizona State University Threatcasting Lab. https://threatcasting.asu.edu/publication/threatcasting-report-information-warfare-and-future-conflict.
13. H. Rothstein, 2007, Strategy and psychological operations. *In Information Strategy and Warfare,* Routledge, 176-202.
14. U.S. Army Training and Doctrine Command, 2018, *TRADOC Pamphlet 525-3-1 the U.S. Army in Multi-Domain Operations 2028*, Fort Leavenworth, KS.
15. S. Tzu, *The art of war* (Vol. 361).
16 B.D. Johnson, 2019, *Information Disorder Machines.* Arizona State University Threatcasting Lab. https://threatcasting.asu.edu/publication/threatcasting-report-information-disorder-machines.
17. U.S. Department of the Army, 2017, *Field Manual 3-0 Operations.* Washington, DC.
18. J.R. Galbraith, 1977, *Organization Design.* Boston, MA: Addison Wesley.
19. U.K. Ministry of Defence. (2019). *Joint Doctrine Note 2/19 Defence Strategic Communication: an Approach to Formulating and Executing Strategy*. Shrivenham, Swindon, Wiltshire.

The Cyber Defense Review

Research Articles

Military Authorizations in a Connected World: DoD's Role in Cyber Influence Operations

Michelle Albert
Tom Barth
Dr. George Thompson

ABSTRACT

The open nature of the Internet, allowing the unprecedented free flow of information, has given rise to a new type of attack surface. Cyber activities in the gray zone, which falls between diplomatic engagement and military action, includes disinformation campaigns and influence operations. These activities raise questions regarding responsibility and proportionate response. This article examines the distinction between influence operations and more traditional conflict, specifically in a gray zone of blended activity. It also addresses the role and authorities of the Department of Defense (DoD) governing cyberspace activity. Deterring and countering adversary influence operations require a multipronged approach of regulation, education, and government agency action to focus agency authorities and resources where they are needed most. DoD has the technical resources to lead the government's efforts to counter and deter such operations but is limited by policy and law. This article considers how DoD can effectively operate under its Title 10 and Title 50 authorities in the gray zone and introduces a heuristic construct for the role of influence operations in the continuum of conflict.

Michelle Albert is a Research Associate in the Information Technology and Systems Division at the Institute for Defense Analyses. Prior to that, she worked as a speechwriter for the Department of Defense Chief Information Officer. She has an M.A. in Journalism.

INTRODUCTION

The global balance of power has changed dramatically in the past two decades. While the US military was focused on the Middle East, Russia and China focused on great power competition, spending considerable time and effort developing substantial cyber capabilities and the supporting doctrines for their use. The US Intelligence Community's (IC) "high confidence" that Russia's Internet Research Agency conducted a sophisticated influence campaign in the run-up to the 2016 US Presidential election[1] informed the public of an Internet-based attack surface that is difficult to understand, categorize, bound, or defend and that presents a rash of new vulnerability risks to US national security.

The open nature of the Internet blurs boundaries and responsibilities. Foreign-led cyber campaigns with a major domestic impact, like Russia's in 2016, create confusion regarding who has the authority to respond. Cyber activities like these occur in the gray zone,[2] which falls between diplomatic engagement and military action and rely on Internet anonymity and the lack of accepted international standards or norms for cyber activity to discourage a conventional military response. Gray zone cyber threats include espionage, threats to critical infrastructure, disinformation campaigns, and influence operations, and originate from foreign and domestic sources. While government responsibilities in the US are traditionally split between foreign and domestic threats and by the type of threat, this split does not directly translate to cyberspace.

This article examines media- and technology-driven disinformation campaigns and influence operations in the context of established trends in military doctrine and gray zone activities. It considers the relationship between influence operations and a traditional state of war, specifically techniques that fall both inside and outside Title 10 authorities for US military activities and Title 50 authorities for intelligence activities.

Tom Barth is a Research Staff Member in the Information Technology and Systems Division at the Institute for Defense Analyses. He previously served as a U.S. Army Infantry officer, with final active duty assignment as Chief, Future Operations, U.S. Army Cyber Command. He is a graduate of the U.S. Military Academy, the U.S. Army Command and General Staff College's School of Advanced Military Studies, and the U.S. Army War College.

This article also addresses those instruments of national power that should be responsible for defending against foreign influence operations.

Doctrine Development in a Changing World

The character of war is subject to change. War is an interaction between communities, and its character depends on the tools and technologies used to shape those interactions.[3] The DoD's *2018 National Defense Strategy* recognizes that the current and future operational environments are "affected by rapid technological advancements and the changing character of war."[4] The microelectronics revolution is central to these technological advancements as it has changed how society collects, manages, and acts on information, both in civilian life and during defense and intelligence activities.

Microelectronics-based technologies have been developed at a rapid pace that far outstrips the development of governing regulatory and usage frameworks in the civilian sector. Predicting new applications of microelectronics is difficult, especially if the applications are disruptive or differ qualitatively from prior applications. The current trend in emerging technologies facilitating the tracking of individual opinions, biases, interests, and beliefs will continue. Recent use of social media to sow discord in targeted populations exemplifies these difficulties.

THE EVOLUTION OF INFLUENCE OPERATIONS

Characteristics of Information Operations and Influence Operations

DoD defines *information operations* as "the integrated employment, during military operations, of information-related capabilities[5] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[6] Military operations include defense support of civil authorities, peace

Dr. George Thompson is a Research Staff Member in the Information Technology and Systems Division at the Institute for Defense Analyses, and previously worked in the semiconductor industry. He has a Ph.D. in Physical Chemistry.

Dr. George Thompson passed away before publication of this article.

operations, noncombatant evacuation, foreign humanitarian assistance, and nation building.[7] Authority to conduct information operations involves a detailed and rigorous legal interpretation of authority and/or the legality of specific actions.[8]

Information operations occur within the *information environment*, which DoD defines as "individuals, organizations, and systems that collect, process, disseminate, or act on information."[9] They also comprise different types of operations. *Psychological operations* involve the use of propaganda to shape the motives and behavior of a government, group, or individuals. *Military deception* uses false information or disinformation to mislead.[10] *Cyberspace operations* involve "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[11] These objectives range from accessing information, to spreading information (or disinformation), to creating some physical effect, such as attacking critical infrastructure. DoD doctrine separates cyberspace operations and information operations, but they are inextricably linked. Cyberspace is where many information operations occur today.

DoD lacks a formal definition of influence operations, which, for purposes of this article, refers to use of information, whether true or false, as propaganda, misinformation (unintentionally false information), and disinformation (intentionally false information) to achieve a desired outcome. According to RAND, *influence operations* refers to the coordinated application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster and promote certain attitudes, decisions, or behaviors in a target audience.[12] Influence operations may take place during either military operations or gray zone activities, and its practitioners reside in military, government, and private sector organizations that cooperate to various extents.

Figure 1, below, highlights the differences between DoD-defined information operations and influence operations. Target audiences range from individuals, to groups, to entire populations, and there are varying methods for reaching an intended target. Influence operations have two main components: the message and the delivery method. One method is the use of regulated mass media, such as TV, newspapers, radio, etc., to reach the broadest possible audience. However, using mass media subjects a message to editing and often creates a means for determining the message's provenance. Another method is to use less regulated means of communication to ensure the message is unadulterated and difficult to trace back to its creators. These means include flyers, posters, word of mouth, postings on social media sites or other message boards, and using anonymizing software such as TOR to hide or obfuscate a user's identity online.[13]

Influence Operations = (Information Operations – Physical Effects) + Misinformation + Disinformation

Figure 1. Information and Influence Operations

Conducting effective influence operations requires thorough knowledge and understanding of the target audience's demographics, ideals, beliefs, attitudes, values, decision-making processes, and receptiveness to information. The source of the information needs to appear authentic and credible to gain the audience's trust, and the information itself must be packaged for maximum appeal.[14] The environment today is saturated with information. To succeed, any influence operations campaign must reach the target audience.

How Technology Has Affected Influence Operations

While the basic tenets of propaganda and influence operations remain the same over time, the Internet has changed how they are employed and how information is presented and consumed. This change is a strategic inflection point in technology development that created a new attack surface for influence operations.

Internet site owners, publishers, and advertisers rely on algorithms that control content seen by users on search engines and social media sites. The algorithms gather as much information about users as possible, including location, age, education, political beliefs, contacts, pop culture preferences, and what posts garner the most likes or activity. The algorithms then tailor content to suit each user's preferences while also considering whether the site was paid to promote a post and how other people in the user's network interact with a post.[15] Personalized content drives continued use of the site, which increases advertising revenues and gives the algorithm even more information. Algorithms are unconcerned whether a post is true, false, innocuous, provocative, or extremist, as long as it fosters engagement.[16]

The Internet's immediacy and ease of access also precipitated the rise of niche publications and blogs that cater to specific audiences. These sites foster communities of people with similar personal identities, interests, hobbies, or ideologies. These online communities are known as "echo chambers," which have become a hallmark of social media sites. Echo chambers, driven

by algorithmic tailoring, validate and amplify an individual's existing beliefs and opinions to the exclusion of narratives that challenge them. It is now easier than ever to find communities of like-minded people online and to be isolated from differing opinions.

THE CURRENT INFLUENCE OPERATIONS ENVIRONMENT

Social Media

Today, 70 percent of Americans use some form of social media.[17] More than half of all social media users use such sites for news, and one in 10 users relies on social media as their only news source.[18] Social media users can pull content they deem interesting or relevant and share it with others, rather than relying on news organizations and publications to push content to them.[19]

This has sparked a rise in citizen journalism. Users not affiliated with a news organization are able to post pictures and video of an event or spread breaking news, providing valuable eyewitness accounts of events as they happen. News of the 2008 attacks in Mumbai, for example, broke over Twitter, with pictures posted to Flickr, a photograph-sharing site.[20] Video, such as the cellphone videos exposing police brutality and racism,[21] has provided evidence for indictments and criminal cases and reshaped national narratives on police behavior and accountability.

False or misleading information, whether mistakenly shared by citizen journalists or deliberately spread to manipulate others, is often more novel than true information, and presented in a manner meant to provoke outrage, which further entices engagement.[22] Also, interacting with false information can lead users to follow algorithmically generated threads known as "rabbit holes."[23] Since the initial search terms are based on false information or unsupported ideas, the algorithm is likely to generate related threads of polarizing information that can incite calls to action in the real world. Increasingly, what happens online has real-world effects. In the summer of 2018, two dozen people in India were killed by lynch mobs because they were suspected of participating in child-kidnapping rings or plots to harvest organs. The mobs were fueled by unfounded rumors spread on WhatsApp, an encrypted messaging Facebook platform.[24]

Twitter has been used to coordinate disaster response efforts, organize grassroots political campaigns, harass journalists and other public figures, foment revolution, and affect jobs. The #MeToo movement revealed episodes of sexual harassment and assault perpetrated by prominent individuals, and in some cases resulted in criminal investigations and trials. The #MeToo movement also sparked a nationwide discussion of harassment, power dynamics, and appropriate behavior in the workplace.

The IC concluded in 2018 that Russia sponsored a major hacking, disinformation, and political ad campaign to interfere in the 2016 US Presidential election. Special Counsel Robert Mueller, who was assigned to investigate Russian interference in the 2016 Presidential election and

possible links between Russian officials and Trump associates, filed indictments charging 35 individuals related to his investigations.[25],[26] Social media are also prime grounds for terrorist group recruitment and radicalization. The Islamic State of Iraq and al-Sham (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL), ran a sophisticated, multifaceted propaganda campaign to glorify its mission and make life under the caliphate seem like paradise.[27] Recruiters used social media to establish relationships with potential recruits, establishing a sense of intimacy and camaraderie to manipulate recruits into joining.[28]

Some recent lone-wolf terrorist attacks, including the plague of mass shootings terrorizing the US, have roots in online communities and social media sites. Some online communities—echo chambers that validate perceived grievances and advocate violence in response—encourage shootings or other violent acts. Dylann Roof, who shot and killed nine African Americans in the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, in June 2015, self-radicalized using white supremacist and neo-Nazi websites.[29] Google's algorithm led him to sites peddling racist propaganda and falsified statistics about black-on-white crime.[30] Roof immersed himself in these sites before committing mass murder.

The Current Environment Renders the US More Vulnerable to Adversary Influence Operations

The continuously expanding Internet creates an ever-growing and ever-changing attack surface. With more people online and more places for them to communicate come more opportunities to spread fake news or narratives meant to manipulate people[31] while increasing mistrust of fact-based media. Mistrust is largely based on perceived bias in the news or of a powerful publication pushing a particular agenda.[32] Political polarization generates mistrust, no matter a publication's commitment to fact checking and other journalistic standards. Many Internet users find it increasingly difficult to distinguish between the opposing poles of factually real news and factually false news. Instead, they believe that the news lies along a spectrum with real news at one end and fake news at the other.[33] Social media algorithms provide an easy conduit for such information. A search that begins with innocuous content can quickly lead to propaganda or even content espousing hate speech or promoting violence. Algorithms are also increasingly able to target small, specific groups of people. The Russian Internet Research Agency's propaganda campaign in 2016 used algorithmic targeting to identify and obfuscate discussions of current issues, recognizing that exploiting existing divisions is easier than creating new ones.

TECHNOLOGY AND THE EVOLVING THREAT

Technology in Today's Information Environment

The current information environment is marked by the confluence of cyber capabilities and influence operations. Artificial intelligence (AI) makes automated programs (bots) appear more human-like, making it difficult to differentiate between real users and bots. Social engineering

campaigns take advantage of human nature and are based on traditional propaganda methods. Many of these methods have become ubiquitous, and many over time have learned how to identify and ignore the most blatant examples. But the recent revolution in data management has changed this paradigm.

Because of the historical, exponential increase in computer functionality for a given cost, the amount of personal data in the public sphere today is unprecedented (and predicted by Moore's Law).[34] In this interconnected world, where almost everyone has a cell phone and is engaged with social media, where most emails are scanned for content, and where records of electronic financial transactions are vacuumed up, digital footprints can be tracked easily by social media and advertising companies seeking profit. Buying or selling data is a lucrative activity. The expansion of semiconductor-based products (e.g., computers, smartphones, and cars) will most likely continue for the foreseeable future, making collection and analysis of digital footprints even more pervasive than it is now.[35]

Nefarious foreign actors have been using some of these data in social engineering and influence operations efforts against the US; Russia's interference in the 2016 US Presidential election is the most prevalent example.[36] Recent advances in AI, image and video analysis, and data mining, combined with the technology of the coming decade, open up the potential for more powerful influence operations. Advanced computing may well enable targeted advertising messages delivered by email or telephone that are indistinguishable from messages sent by humans, and use detailed psychological profiles to tailor messages to specific targets.

Technology today can be divided into three frameworks: sensing, processing, and acting. Sensing relates to the means for gathering data. Processing is both storing and accessing the data and analyzing those data to discover and extract useful information. Acting relates to how that information is used. Cyberspace is littered with sensors, even to the extent of tracking users as they read. That information is then rapidly processed and added to the users' existing online profiles, which strongly influence what articles and advertisements users are steered toward.

Data collection and analysis can instigate and influence action, such as in boosting security, preventing criminal activity, or tracking disease outbreaks. Data mining and analytics tools such as Palantir[37] collect information from emails, financial documents, phone records, and other sources to search for potential links. Palantir has been used to predict the deployment of improvised explosive devices (IED), detect fraud, conduct criminal investigations, track complex financial transactions, and screen airport travelers. Tools like Palantir have been a boon for security organizations, but they also present risks and challenges, partly because they lack a mechanism to determine the validity of collected information, which may affect the tool's predictions. Incorrect and misleading information collected in Palantir has resulted in mistaken arrests.[38]

The Future Environment

The global trend toward universal surveillance will continue as more technologies track our activity online and offline. Increased networking and data collection expand the potential attack surface. More data mean more information about potential targets and target groups. More online systems mean more access points to exploit. A society's surveillance capability, either government or private sector, could be weaponized and used against it for a cyberattack or influence operations campaign.

It will become increasingly difficult to determine authenticity of information online. Audio and video recordings provide an eyewitness view into events and have corroborated or invalidated witness accounts of what actually happened. Moreover, it is becoming easier to create faked audio and video that are almost indistinguishable from the real thing. Known as *deepfakes*, these audio and video clips enable malicious actors to make it seem like someone did or said something that he or she never did or said, opening up myriad avenues for disinformation.[39] A very common type of deepfake today is the grafting of a celebrity's head onto a porn actor's body. However, it would be an easy transition to deepfakes meant to destroy reputations, rig elections, erode trust in public institutions, and jeopardize national security.

There is no single answer or method for employing defensive measures against the risks of this future environment. Increased connectivity brings greater risk, and each organization or individual accessing networked systems and resources must weigh the desire for convenience against the need for privacy and security. Addressing future risks and opportunities requires both government and private sector participation, and a multi-pronged approach of legislation, regulation, education, and government agency action. Broad regulation is a government responsibility that may require restricting dissemination of online information. Education and media literacy campaigns can arm the public with tools that help flag disinformation and help people think more critically about what they are seeing. Stopping current campaigns and deterring new ones also require further action. A whole-of-government approach to fighting disinformation, coupled with public and private sector collaboration, will focus authorities and resources where they are needed most. DoD has the technical resources to lead such an effort but is limited by policy and law. Partnering with other agencies and private organizations will likely enable the DoD to provide cyber capabilities and expertise when and where needed.

ADDRESSING THE CURRENT THREAT

DoD's Role

The *2018 National Defense Strategy* recognizes that the US military must operate in "an increasingly complex global security environment" and use "areas of competition short of open warfare (e.g., information warfare, ambiguous or denied proxy operations, and subversion)" to achieve our ends.[40] To counter coercion and subversion in competition short of conflict, DoD supports US Government (USG) interagency efforts and works by, with, and through allies and

partners to secure national interests.[41] Such a strategic approach suggests DoD either does not or should not have a leading role in the government's efforts to counter adversary information operations, save for information operations that directly target US forces.

Title 10 and Title 50 Authorities

Titles 10 and 50 of the U.S. Code refer to statutory authorities governing DoD and the IC. Title 10 delineates the functions, duties, and responsibilities of the US military and gives the Secretary of Defense (SECDEF) control over all DoD agencies and commands. It also establishes the combatant commands (COCOM) and gives them statutory authorities, which all report directly to the SECDEF.[42] Title 50 establishes the IC's authorities, and constitutes CIA's authority to conduct intelligence operations and covert actions. Title 50 also establishes Secretary of Defense control over intelligence agencies within DoD, including NSA and the Defense Intelligence Agency (DIA).[43]

While both are subject to Congressional oversight, one difference between Titles 10 and 50 is the need for Congressional notification. Title 10 activities are overseen by the House and Senate Armed Services Committees (HASC and SASC, respectively), and Title 50 activities are subject to oversight by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).[44] Nevertheless, Title 50 IC activities require advance notice to Congress, while military activities under Title 10 do not.[45] Another key difference is international protection of sovereignty. Intelligence agencies operating outside the US in covert action status under Title 50 have reasonable claim to international law protection of sovereignty because covert action status carries a statutory obligation to comply with the Constitution and US statutes, but nothing else. Title 10 does not carry the same "implicit statutory shield" against international law objections.[46]

Questions of oversight and responsibility arise when actions could reside under either Title 10 or Title 50. Historically, Congress and executive agencies have viewed Title 10 and Title 50 as separate entities. Yet these Titles themselves, as well as Secretary of Defense authorities under both, suggest otherwise. Some activities fall under either Title, depending on their command and control, funding, and mission intent.[47] IC and DoD both conduct intelligence gathering, generally viewed as falling under Title 50, but intelligence gathering is included under both Title 10 and Title 50. The SECDEF can direct DoD organizations and personnel to execute intelligence activities. Activities meant to fulfill national intelligence requirements fall under Title 50, and if they meet military intelligence requirements, or are used to prepare for an organized conflict, they fall under Title 10. Military intelligence operations in support of taskings from the Director of National Intelligence (DNI) fall under Title 50 and must be reported, but intelligence activities in support of SECDEF taskings are considered Title 10. Furthermore, activities by DoD entities that are also members of the IC fall under both Titles 10 and 50.[48]

In modern operations, particularly in cyberspace operations, convergence of Titles 10 and 50 activities becomes more apparent. Exploiting a network or system to gather information but not to alter, control, or degrade the function of that network or system is generally considered

an intelligence activity, and international law does not consider intelligence activities to be acts of war. On the other hand, exploiting a network or system in order to alter, control, or degrade its function surpasses that threshold and is more likely to be subjected to international law constraints.[49] (In the gray zone, rules of engagement for US cyber operations remain fuzzy and undefined.[50]) Yet, cyber operations often require intelligence gathering to assess a network or system in preparation for an attack. Moving from one activity to another—from Title 50 to Title 10—especially when operating in a foreign country, exposes potential international law issues. Part of the challenge is that cyberspace operations often happen quickly: a fleeting opportunity may arise, that cannot await legal authorization, especially if foreign governments need to consent.

Title 10-Title 50 convergence also raises questions as to who is responsible for intelligence gathering and other cyber operations. The United States Cyber Command (USCYBERCOM), the unified combatant command responsible for cyberspace operations, partners with NSA. The Commander, USCYBERCOM, is also the NSA Director, thereby underscoring the ties between the two organizations. Historically, NSA has been the USG's lead for cyber operations, but USCYBERCOM's responsibility and authority are growing. Convergence is complicated for cyber operations and is even more complicated for information operations.

Current Activities

The 2019 National Defense Authorization Act (NDAA) expanded USCYBERCOM's statutory authorities.[51] The NDAA modifies parts of Title 10 to empower the DoD to conduct cyber operations short of hostilities[52] and in areas where "hostilities are not occurring,"[53] and defines clandestine military activity in cyberspace as "a traditional military activity."[54] The designation of clandestine online activity as traditional military activity removes the oversight required by Title 50. The NDAA also empowers USCYBERCOM to conduct cyber operations that respond to foreign country cyberattacks, but only if those attacks meet two conditions: they constitute "an active, systematic, and ongoing campaign of attacks against the USG or people of the US in cyberspace, including attempting to influence US elections and democratic political processes."[55] Section 1642 of this NDAA restricts this authority to respond to attacks coming from Russia, North Korea, China, or Iran.[56]

USCYBERCOM's actions to protect the 2018 US midterm elections and the 2020 Presidential election, both the subject of repeated foreign adversary attacks, could provide a framework for how the DoD fights disinformation. In each election cycle, USCYBERCOM worked with other combatant commands, such as the Department of Homeland Security (DHS), the Department of the Treasury, and the FBI, and partnered with allied nations to find instances of foreign interference in the election process.[57] To combat 2018 midterm disinformation, USCYBERCOM and NSA created the Russia Small Group task force to deter and protect against Russian disinformation and cyberattacks.[58] On election day, the task force blocked Internet access to the Internet Research Agency in St. Petersburg, long identified as the locus of Russia's disinformation campaign against the US.[59] The task force has since been made permanent.

Creating a Cybersecurity Agency

Another way to counter and deter disinformation would be to create a single government cybersecurity agency. The acknowledgment of cyberspace as a warfighting domain and the intricacies of its related attack surface suggest a need for a new agency focused on this particular threat. Agencies that must fulfill other traditional responsibilities and missions may, with the newer cyber-related missions, be stretched thin. A single, focused, cybersecurity agency that consolidates law enforcement, intelligence activities and the authorities related to cyber activity from both foreign and domestic sources could be more agile and mission-focused, and thereby serve as a hub for top cybersecurity talent. This agency would lead all cyber-focused activities and support other agencies as needed.[60]

Promoting partnerships among existing government cyber resources may advance collaboration among agencies and strengthen existing relationships with the private sector, which has a larger bench of cybersecurity talent and owns the most influential Internet platforms (e.g., Facebook, Twitter, Amazon). This would also facilitate relationships with key government personnel from affected sectors that have no cybersecurity-focused missions. USG cyber expertise today is spread among agencies, with some overlap in mission—for example, intelligence centers such as the Defense Cyber Crime Center (DC3) and the Cyber Threat Intelligence Integration Center, where agency-specific cyber resources can develop specialized skills tailored to specific missions. Increased collaboration among these resources would provide support when and where needed, without the extra cost and upheaval of establishing a new agency.[61] Today, the Authorities that handle domestic or foreign threats are split up among agencies. Combining these authorities into a new agency would mirror the current confusion regarding Title 10 and Title 50 convergence within DoD. The IC and law enforcement agencies separately are dedicated to domestic and foreign activities. Combining these disparate authorities at best would be challenging.

Adopt a Heuristic Construct for Conflict

The onslaught of foreign surveillance into US critical infrastructure and intrusions into social media takes us beyond the question: "How do we deal with these intrusions?" to the question: "Are we at war, and we did not realize it?" Prussian war theorist Carl von Clausewitz argued that the nature of war describes its unchanging essence, and the character of war describes how as a phenomenon it manifests in the real world. War's nature is violent, interactive, and fundamentally political. War's conduct is influenced by technology; law; ethics; culture; methods of social, political, and military organization; and other factors that change across time and place.[62] Understanding the complexity and differences among the various approaches to warfare is critical for understanding adversaries, their methods, and their concepts for victory. US military doctrine so far has successfully evolved to meet the challenges of conventional warfare, irregular warfare, and terrorism. This evolution must continue.

By definition, a hallmark of all gray zones is a blurring of boundaries and responsibilities. The new battle space spans the public and private sectors and encompasses media outlets, social media sites, a range of technologies, and individual citizens. What constitutes a cyberspace attack is yet to be concretely defined (perhaps excepting cyberattacks that cause physical effects). Consequently, it is difficult to determine a response acceptable under international law to incursions into US networks, even when the effects of such incursions have been profound. This new warfare domain does not neatly adhere to current doctrinal definitions. To embrace the changing conduct of war, the US military should adopt a heuristic construct for conflict—as depicted in Figure 2—and abandon any binary peace/war distinction.[63]

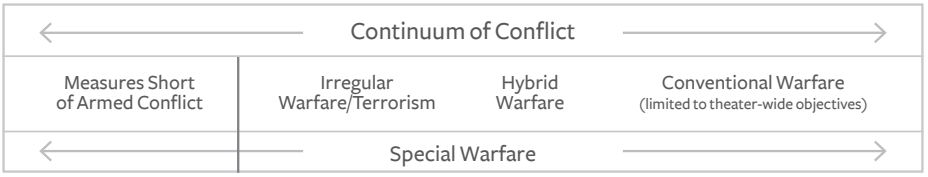


Figure 2. Continuum of Conflict [64]

Given the nebulous nature of the gray zone, it is difficult to define the battle space, much less victory, in the context of influence operations. In fact, the concept of victory might better be stated as maintaining an advantage. Battling influence operations campaigns requires a three-pronged approach of regulation, education, and public-private collaboration. Broad regulation is a government responsibility; that social media companies operating in Europe are already complying with European Union (EU). regulations shows that it is feasible that they can comply with similar US regulations.[65] Education and media literacy campaigns give the public tools to help identify disinformation and think critically about the information they see and interact with online. However, it is not enough to arm the public with the knowledge of these campaigns; we need to stop current campaigns and prevent new ones.

Doing so would require the USG's involvement and a collaborative approach with the private sector. Individual agencies have particular areas of focus and responsibility, and a whole-of-government approach to fighting disinformation would focus agency resources and expertise where they are needed most. DoD has the resources and abilities to take the technical lead but is limited by policy and law. Partnering among DHS, FBI, and other agencies would enable DoD to provide cyber capabilities and expertise where needed, and this must continue and expand. DoD partners with the Department of State's Global Engagement Center, which is charged to "lead, synchronize, and coordinate efforts of the federal government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining US national security interests."[66] USCYBERCOM and NSA's Russia Small Group task force, as well as USCYBERCOM's partnerships with allied nations and US government agencies, present a model for future DoD involvement in blunting disinformation. USCYBERCOM's Joint Task Force Ares has partnered with NSA to act as a hub for whole-of-government cyber planning.[67]

USCYBERCOM's pre-authorization to conduct cyber operations against cyberattacks from certain foreign countries defines a proportionate response in specific instances. Establishing that the US can and will respond to an attack is part of an effective deterrent, but defense requires a different approach. Effective defense against influence operations requires the Secretary of Defense to exercise both Title 10 and Title 50 authorities. In the gray zone, questions for DoD are how to operate under these authorities, and when to use them. It may be that finding a means of straddling domestic and foreign activities—like the Coast Guard's jurisdiction covering both domestic and international waters—would be an effective approach, as foreign-led disinformation campaigns, such as Russia's in 2016 and 2018, often spur domestic action online and in the real world.

CONCLUSION

Today we are in a reactive state, scrambling to keep pace with technology and respond to its effects. In the microelectronics arena, new and unforeseen applications of rapidly evolving technology are commonplace. It is not uncommon for new technologies or new applications of existing technologies to create a temporary advantage for innovators and early adopters while defensive technologies, policy, and doctrine adjust.

The limitations and constraints expressed in policy and in DoD's military doctrine make it difficult to incorporate DoD in a whole-of-government response to adversary influence operations in an environment short of war. For DoD, information operations are key to winning the battle of the narrative, which pits adversary attempts to influence the perception of different populations against US efforts to do the same.[68] The battle of the narrative is an integral part of irregular warfare and requires creating a coherent message, working with the host nation or local partner to boost their legitimacy, disseminating the message to the local population and other key audiences, and delegitimizing the adversary's message and goals.[69]

The battle of the narrative, however timeless, is applicable beyond irregular warfare. The emergence of the gray zone and the blurring of what constitutes wartime and peacetime activity have instigated a constant battle to control the narrative and influence the ideas and actions of target populations. To respond to adversary influence operations short of conflict, DoD will need to be imaginative within the bounds of law, policy, and capabilities to integrate information operations and cyberspace capabilities to counter and contest its adversaries globally.[70]

The capability to prevent, contest and prevail in influence operations campaigns needs to become a national priority. Special Counsel Robert Mueller's testimony to the House Judiciary and Intelligence Committees on July 24, 2019 issued a warning about election interference: the 2016 election interference "wasn't a single attempt. They're doing it as we sit here."[71] Election interference and other influence operations campaigns are going to continue to expand in scope and affect our society and way of life.

NOTES

1. Intelligence Community Assessment (ICA), January 6, 2017, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
2. The gray zone refers to "employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces" (International Security Advisory Board (ISAB,) January 3, 2017, *Report on Gray Zone Conflict*, https://www.state.gov/documents/organization/266849.pdf).
3. Z.T. Brown, March 12, 2019, "Unmasking War's Changing Character," Modern War Institute, https://mwi.usma.edu/unmasking-wars-changing-character/.
4. Department of Defense, 2018, *Summary of the 2018 National Defense Strategy of the United States of America*, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
5. *An information-related capability* (IRC) is a "tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions," Joint Publication 3-13, November 27, 2012, *Information Operations*, incorporating Change 1, November 20, 2014.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. C.A. Theohary, March 5, 2018, CRS Report 7-7500, "Information Warfare: Issues for Congress," Congressional Research Service.
11. Joint Publication 3-12, June 8, 2018, *Cyberspace Operations.*
12. E.V. Larson, et al., 2009, "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," RAND, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.
13. Ibid.
14. Ibid.
15. A. Hern, May 22, 2017, "How social media filter bubbles and algorithms influence the election," *The Guardian*, https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles.
16. M. Fischer and A. Taub, April 25, 2018, "How Everyday Social Media Users Become Real-World Extremists," *The New York Times*, https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html.
17. A. Perrin and M. Anderson, April 10, 2019, "Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018," Pew Research Center, https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.
18. S. Bradshaw and P.N. Howard, January 29, 2018, "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life," *Knight Foundation*, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.
19. Ibid.
20. C. Beaumont, November 27, 2008, "Mumbai attacks: Twitter and Flickr used to break news," T*he Telegraph*, https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.
21. G. Denby, October 18, 2014, "Videos of Deadly Police Encounters Grab the Media Spotlight, but Why?" *NPR*, https://www.npr.org/blogs/codeswitch/2014/10/08/354507430/videos-of-deadly-police-encounters-grab-media-spotlight.
22. S. Vosoughi, D. Roy, and S. Aral, March 9, 2018, "The spread of true and false news online," *Science,* 359, 1146-1151.
23. The term "down the rabbit hole" originated with Lewis Carroll's book *Alice in Wonderland*, in which Alice falls into and down a rabbit hole that eventually leads her to Wonderland. Today, the term "rabbit hole" refers to "a complexly bizarre or difficult state or situation conceived as a hole into which one falls or descends," especially "one in which the pursuit of something (such as an answer or solution) leads to other questions, problems, or pursuits, " "rabbit hole," *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/rabbit%20hole, accessed October 1, 2019.
24. E. Dwoskin and A. Gowen, July 23, 2018, "On WhatsApp, fake news is fast—and can be fatal," *The Washington Post,* https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html?noredirect=on&utm_term=.05a5faed4172.

NOTES

25. Department of Justice Office of Public Affairs, February 16, 2018, "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.
26. M. Kahn, July 13, 2018, "Document: Special Counsel Indicts 12 Russian Intelligence Officers for Hacking DNC and Clinton Campaign," *Lawfare*, https://www.lawfareblog.com/document-special-counsel-indicts-12-russian-intelligence-officers-hacking-dnc-and-clinton-campaign.
27. B.I. Koerner, 2016, "Why ISIS Is Winning the Social Media War," *Wired*, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/#slide-5.
28. A. Erelle, June 2, 2015, "How One Journalist Found Herself Courted by ISIS," *Vogue,* https://www.vogue.com/article/in-the-skin-of-a-jihadist-isis-recruitment-network-excerpt-anna-erelle.
29. C. Collins, 2017, "The Miseducation of Dylann Roof," *Teaching Tolerance*, https://www.tolerance.org/magazine/fall-2017/the-miseducation-of-dylann-roof.
30. Ibid.
31. J. Anderson and L. Rainie, October 19, 2017, "The Future of Truth and Misinformation Online," Pew Research Center, http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/.
32. N. Newman and R. Fletcher, 2017, "Bias, Bullshit and Lies: Audience Perspectives on Low Trust in the Media, Digital News Project 2017," Reuters Institute for the Study of Journalism and University of Oxford, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-11/Nic%20Newman%20and%20Richard%20Fletcher%20-%20Bias%2C%20Bullshit%20and%20Lies%20-%20Report.pdf.
33. Ibid.
34. G.E. Moore, April 19, 1965, *Electronics*, Vol. 38, No. 8.
35. There are arguments that the scaling predicted by Moore's Law may be ending in the next decade, but the industry has already begun the research and development into alternate architectures and technology to continue scaling without necessarily continuing to decrease the dimensions of the actual semiconductor.
36. E. Dwoskin, C. Timberg, and A. Entous, October 2, 2017, "Russians took a page from corporate America by using Facebook tool to ID and influence voters," *The Washington Post*, https://www.washingtonpost.com/business/economy/russians-took-a-page-from-corporate-america-by-using-facebook-tool-to-id-and-influence-voters/2017/10/02/681e40d8-a7c5-11e7-850e-2bdd1236be5d_story.html.
37. "Why We're Here," Palantir, https://www.palantir.com/about/.
38. P. Waldman, L.Chapman, and R. Robertson, April 19, 2018, "Palantir Knows Everything About You," *Bloomberg*, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.
39. R. Chesney and D. Citron, 2019, "Deepfakes and the New Disinformation War: The Coming Age in Post-Truth Geopolitics," *Foreign Affairs*, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.
40. Summarized from the 2018 National Defense Strategy Summary, 2-3.
41. Summarized from the 2018 National Defense Strategy Summary, 5.
44. 10 U.S.C. §§ 101-18525.
43. 50 U.S.C. §§ 1-2420.
44. A.E. Wall, 2011, "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal,* Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.
45. Ibid.
46. R. Chesney, April 12, 2018, "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries," *Lawfare*, https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.
47. A.E. Wall, 2011, "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal*, Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.
48. Ibid.
49. Ibid.

NOTES

50. C. Bing, April 11, 2018, "Command and control: A fight for the future of government hacking," *cyberscoop,* https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.
51. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).
52. 10 U.S.C. § 394(b).
53. Ibid.
54. 10 U.S.C. § 394(c).
55. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).
56. Ibid.
57. C.T. Lopez, May 14, 2019, "Persistent Engagement, Partnerships, Top Cybercom's Priorities," Department of Defense, https://www.defense.gov/Newsroom/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.
58. P.M. Nakasone, February 14, 2019, Statement before the Senate Committee on Armed Services.
59. E. Nakashima, February 27, 2019, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on.
60. A. Burt and J.C. Trainor, January 2, 2020, "Our Government's Approach to Cybersecurity Is a Costly Mess. Here's What Would Fix the Problem," Time, https://time.com/5757811/cybersecurity-attacks-agency/.
61. S.C. O'Connell, January 29, 2020, "We don't need a separate cybersecurity agency," Politico, https://www.politico.com/news/agenda/2020/01/29/dont-need-separate-cybersecurity-agency-106631.
62. C. Mewett, January 21, 2014, "Understanding War's Enduring Nature Alongside Its Changing Character," War on the Rocks, https://warontherocks.com/2014/01/understanding-wars-enduring-nature-alongside-its-changing-character/.
63. F.G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism 7,* No 4, https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.
64. Adapted from reference 61.
65. P.M. Lefkowitz, June 25, 2019, "Why America Needs a Thoughtful Federal Privacy Law," *The New York Times*, https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html?searchResultPosition=2.
66. National Defense Authorization Act (NDAA) for Fiscal Year 2017, Pub. L. 114-328 § 1287(a)(2).
67. P.M. Nakasone, February 14, 2019, Statement before the Senate Committee on Armed Services.
68. Department of Defense, May 17, 2010, *Irregular Warfare: Countering Irregular Threats Joint Operating Concept Version 2.0*, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.
69. Ibid.
70. How the Department of Defense will need to respond was taken from the USCYBERCOM 2018 *Cyberspace Strategy Symposium Proceedings*, p. 2.
71. Davis J. Hirshfeld Davis and M. Mazzetti, July 24, 2019, "Highlights of Robert Mueller's Testimony to Congress," *The New York Times*, https://www.nytimes.com/2019/07/24/us/politics/mueller-testimony.html?action=click&module=RelatedLinks&pgtype=Article.

Causal Reasoning with Autonomous Systems and Intelligent Machine Applications

Dr. Rusty Baldwin
Dr. Harold J. Arata III

ABSTRACT

In the field of Artificial Intelligence (AI), Machine Learning (ML) techniques and algorithms have been employed in a wide variety of domains and have demonstrated incredible capabilities as well as continued applicability to an ever-expanding number of areas and applications. Image and speech recognition, medical diagnosis, classification and prediction, information extraction (i.e., deep learning), commercial market and customer analysis, robotics, and self-driving vehicles are a few of the many areas where ML has either made possible or had a significant impact. Yet for all this progress, the field of AI has not yet approached what many consider the holy grail of AI: machines with human-like intelligence. Causal analysis is essential for realizing the vision of human-like reasoning: it brings the ability to determine cause-effect relationships and provides a basis for reasoning about interventions (i.e., doing), as well as what might have happened had events occurred differently (i.e., imagining/retrospection) which are fundamental characteristics of human reasoning. Causal analysis has seen widespread use and success in epidemiology, social science, and other fields for decades. Even so, its use in engineering, computer science, and AI has been limited and its potential is just beginning to be widely recognized and applied.

Dr. Rusty Baldwin is a Distinguished Research Professor in the Computer Science Department of the University of Dayton. He received a B.S. in Electrical Engineering (cum laude) from New Mexico State University in 1987, an M.S. in Computer Engineering from the Air Force Institute of Technology in 1992, and a Ph.D. in Electrical Engineering from Virginia Polytechnic Institute and State University in 1999. He served 23 years in the United States Air Force and retired in 2004. He is a registered Professional Engineer in Ohio and CISSP. He is a member of the Fellowship of Catholic Scholars, Eta Kappa Nu, Tau Beta Pi, and the Association for Computing Machinery. He has published over 100 journal and conference papers in various areas and is co-inventor on 3 patents and 7 USAF inventions. His research interests include resilient and trusted systems, autonomous systems, cyber security, computer communication networks, embedded and wireless networking, and side channel analysis.

INTRODUCTION

In the field of Artificial Intelligence (AI), Machine Learning (ML) techniques and algorithms have been employed in a wide variety of domains and have demonstrated incredible capabilities as well as continued applicability to an ever-expanding number of areas and applications. Image and speech recognition, medical diagnosis, classification and prediction, information extraction (i.e., deep learning), commercial market and customer analysis, robotics, and self-driving vehicles are a few of the areas that ML has either made possible or has had a significant impact on. The success of ML is indisputable and will continue to be an important technology for the foreseeable future.

Two grainy film shots taken at Bell Laboratories in 1952, highlight mathematician and Bell Labs researcher Dr. Claude Shannon's own construction of a robotic, maze-solving mouse known as Theseus, one of the world's first examples of machine learning (Figure 1).

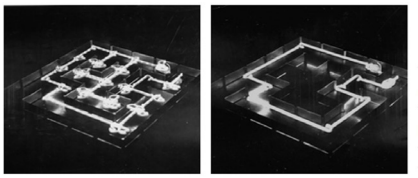
The Theseus of ancient Greek mythology navigated a minotaur's labyrinth and escaped by following a thread given to him by Mino's daughter, Ariadne, which he had used to mark his path. But Shannon's electromechanical marvel was able to "remember" its path with the help of telephone relay switches.[1]

Shannon's wheeled mouse methodically explored its surroundings—a 25-square maze. Shannon tells viewers that the maze's metal walls can be freely rearranged, so Theseus must use a small computing machine to learn the layout anew each time. But the mouse, a tiny wooden device containing a bar magnet and adorned with wire whiskers, is far too small to contain a computing machine. Instead, the machinery is hidden beneath the floor of the maze, a series of telephone relay circuits he has repurposed to do something that they had never done before: learn.[1]

Theseus was also ahead of its time, and "inspired the whole field of AI," says Dr. Mazin Gilbert, who

Dr. Harold J. Arata III, CISSP, is the Lead Systems Design Engineer at AT&T, supporting AT&T National Security and Defense. He has earned six university degrees, including a Ph.D. in computer science from the University of Tulsa. Most recently, Dr. Arata served as an Executive for Cybersecurity Strategy at Hewlett Packard Enterprise (HPE). Preceding his career in industry, Dr. Arata was the Director of the Air Force Cyberspace Technical Center of Excellence, Air Force Institute of Technology (AFIT), where he educated 650 joint cyber professionals a year. Dr. Arata also served as a Senior Military Professor at AFIT, conducting defense-focused research at the Master's and Ph.D. levels. Preceding Dr. Arata's federal civil service, he was an active duty, 2-year, below-the-zone, select to Full Colonel. Dr. Arata's military awards include being individually designated Best-in-Air Force as the Lt. General Leo Marquez Communications-Electronics award winner and being a recipient of the Legion of Merit.

was the Vice President of Advanced Technology with AT&T Laboratories. The mouse, who was featured in *Popular Science*, *Time*, and *Life* magazines the same year the film was made, learned purely through trial and error. Dr. Gilbert explained that "this random trial and error is the foundation of artificial intelligence."[1]



These photos, published in Life magazine in 1952, show the path Theseus took while learning a maze pattern and the direct path taken on its second trip through the same maze.

Figure 1: Theseus in Action[1]

Although there has been much progress made in AI since Theseus, the field of AI has not yet approached what many consider the holy grail: machines with human-like intelligence. In the 1950's, Alan Turing developed what became known as the "Turing Test" to determine if a machine had achieved intelligence. If an evaluator cannot tell whether they are interacting with a human or a machine over a text-only channel, the machine is said to have passed the test.[2] Whether the Turing Test is sufficient to demonstrate human-like intelligence has long been debated. What is not debatable is that systems exhibiting some level of intelligent behavior as well as the ability to learn complex and increasingly sophisticated tasks have been developed for decades. However, many feel this progress has plateaued and has failed to reach human-like intelligence.

A prominent voice in the AI community and the developer of Bayesian networks, Judea Pearl,[3] maintains that the ability to determine and reason about causality (i.e., cause and effect) is fundamental to human intelligence because it allows one to answer the question, "why?" Current ML techniques and algorithms cannot reach this level of inquiry because they are largely based on discovering associations in data (i.e., correlation) based on the passive observation of a system or post-hoc data analysis. This approach limits what can

be achieved; it cannot determine cause-effect relationships because, fundamentally, ML algorithms use what statisticians call observational data. Observational data, except when carefully collected via randomized controlled experiments, cannot be used to uncover cause-effect relationships. What Pearl has dubbed the New Science of Cause and Effect[4] or causal analysis, is the ability of AI to determine cause-effect relationships from observational data under modest conditions in which actual systems operate. Furthermore, causal analysis provides the basis for reasoning about the effect of changing aspects of system operation without actually doing it (i.e., interventions), as well as reasoning about what might have happened had events occurred differently (i.e., imagining/retrospection). Causal analysis has had widespread use and success in epidemiology, social science, and other fields for over a decade.[4][5][6][7]

Its use in engineering, computer science, and AI, however, has been limited and its potential is just beginning to be widely recognized and applied. The background section that follows briefly discusses why typical inference systems (e.g., those using $1^{st}/2^{nd}$ order logic or constraint satisfaction) and data analysis alone is insufficient to determine causal relationships.

Background

Predicate and propositional logic has long been used to allow AI to reason about various combinations of propositions and the relations between them, as well as to determine whether a logical formula is true over a particular logical element or range of elements in the domain under consideration. This and other higher order logic systems constitute a fundamental basis for inference in computer science, mathematics, and other areas of science. They are essential and irreplaceable. Nevertheless, they do not provide a sufficient foundation for reasoning about cause and effect.

Consider as a simple example a naïve application of the chain rule which infers a conclusion from a set of implications. The chain rule for two implications can be shown symbolically as: $A \rightarrow B, B \rightarrow C \therefore A \rightarrow C$ or if A then B, if B then C, therefore if A then C. Though the conclusion is valid and the propositions are true, this type of reasoning fails to correctly assess causality when applied to ordinary everyday situations which even a child would be able to assess correctly. For when the symbols are said to represent actual objects the results can be nonsensical. For instance, let $A \rightarrow B$ be, "If we break the bottle, the grass will get wet." Let $B \rightarrow C$ be, "If the grass is wet, then it rained." An application of the chain rule would then produce $A \rightarrow C$, "If we break the bottle, then it rained." While simplistic, this example illustrates a fundamental limitation of many logic systems that are restricted to manipulating symbols. Causal or common-sense relationships between propositions cannot be specified because all propositions, as propositions, are interchangeable. This equivalence of propositions is what gives these kind of logic systems wide applicability but simultaneously limits their usefulness in causal analysis.

Consider another reasoning approach that had its genesis in AI and operations research: constraint satisfaction. Constraint satisfaction finds feasible solutions to achieve specified goal(s) under a given set of constraints while considering the capabilities of the agent(s) and

the problem domain. The following example,[8] illustrates this approach. Suppose we have a suitcase with two locks: one on the left and the other on the right. The state of the suitcase, open or closed, depends on the position of the locks as shown in Table 1. If both locks are open the suitcase will open (#1), otherwise the suitcase will remain closed (#2-4). The constraint to be satisfied is the suitcase remaining closed. Consider the case where the suitcase is in state #2, the left lock is closed and the right lock is open. A query submitted to the constraint satisfaction system asks, "What would happen if the left lock were also opened?" This is a causal question and should result in the answer that the suitcase would open (#1). However, the response received from the constraint satisfaction inference engine was, "The right lock might get closed." Clearly an incorrect assessment of what should result! The reason for this is such systems are designed to ensure the specified constraint(s) are maintained, not to assess common sense causal effects.

Table 1: Suitcase State

	Left Lock	Right Lock	Suitcase
1.	Open	Open	Open
2.	Closed	Open	Closed
3.	Open	Closed	Closed
4.	Closed	Closed	Closed

Finally, consider a system from which we can observe/collect binary information from five entities labelled A through E that constitute the system as shown in Table 2.[4] The goal is to determine whether there is a causal relationship between entities A and E. That is, does A *cause* E? Clearly A is correlated with E (and with B, C, and D). In fact, all the pairwise entities are correlated. Equally clear is that additional data (given they remain all 0's or 1's) will not help clarify the situation. Causality cannot be determined in this situation because, as every Statistics 101 student learns, correlation does not *necessarily* imply causation. The fact remains, though, that the converse *is* true. Causation necessarily implies correlation. Human reasoning exploits this fact in the quest for knowledge and in search for the answer to the question, "why?"

Table 2: Binary System Data

Entities				
A	B	C	D	E
1	1	1	1	1
0	0	0	0	0
1	1	1	1	1
1	1	1	1	1
0	0	0	0	0
0	0	0	0	0
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1

Vision and Objectives

The vision described here is a lofty one: to enable human-like reasoning (i.e., cognition/common sense) in Autonomous Systems (AS) and Intelligent Machines (IM). Achieving this vision will require the ability to make causal inferences and engage in causal reasoning in near real-time. The objective of this article is to take the next logical step towards enabling this vision by developing a Causal Reasoning Framework (CRF) that will provide the foundational framework and capability for causal reasoning.

Causal Reasoning

Causal reasoning is not complicated. Causal reasoning begins implicitly or explicitly every time the question, "why?" is asked. People want to know the cause of what happens; they inherently want to understand reality. "Why did this person die from lung cancer and that person live?"; "Why was this product profitable and that product a failure?"; "Why didn't the firewall protect the network?"; "Why do rocks drop down instead of up?" Because causal reasoning is the ordinary method of inquiry for human beings, we typically do not even think about it.

Reasoning is more formal in the fields of science and engineering, but the end goal is the same: to answer the question, "why?" The typical approach is to systematically sample a population or system of interest, ***P***, and analyze the sample data as depicted in Figure 2. Statistical inference based on this sample data allows conclusions to be drawn about properties of ***P*** being measured, ***Q(P)*** at some level of confidence. This statistical inference process is sample data-centric.

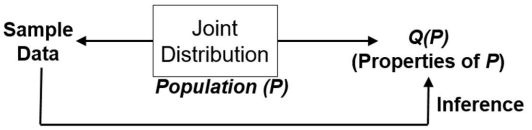


Figure 2: Statistical Inference[9]

As shown in Figure 3, the focus in causal inference shifts from ***P*** to the causal model ***M***, where the joint distribution of the data that comprises ***P*** is generated. That is, the goal of causal inference (as distinct from statistical inference) is to discover the causal model ***M*** that produced ***P.*** As Figure 3 indicates, sample data still plays a critical role in that it is used to make inferences about the properties, ***Q(M),*** of ***M***. But as will be shown, with ***M*** one can now reason about the effect on ***P*** of interventions (i.e., the effect of changing ***M***) or given that ***M*** is known or has been discovered, one can reason about what would have happened if ***M*** had been different even in the absence of any sample data from ***P***. Causal models are not data models, they are reality models.[4]

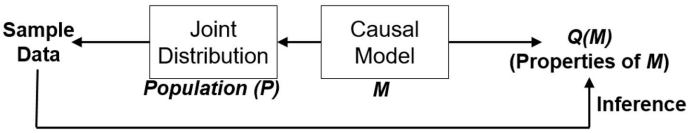


Figure 3: Causal Inference[9]

Pearl has developed a model of human reasoning that he calls the Ladder of Causation.[4] At the bottom rung of the ladder is *Association* whereby the probability of observing y given x was observed or $P(y|x)$ is ascertained. This corresponds to the human activity of observation. These probabilities are ascertained via data collection (i.e., passive observation). Except for the specialized case of randomized controlled experiments which are specifically engineered to uncover causal relationships, almost all of ML uses passive observation to produce its results by calculating conditional probabilities of an event at a given level of confidence. Typical questions that can be answered at this rung of the ladder include: "What does a symptom (x) tell me about a disease (y)?" or "What does sales data (x) tell me about my customer (y)?"

The next rung up the ladder is *Intervention*. This corresponds to the human activity of doing. Under intervention, the experimenter is no longer a passive observer but actively changes the data generating process M. With intervention, the probability of observing y given I *do* $\mathbf{x}$ or $P(y|\mathbf{do}(x))$ is ascertained. The operator, $\mathbf{do}(x)$, signifies Pearl's do-calculus[3] has been applied. The **do** operator is one of the most significant results of Pearl's causal research because it enables one to use observational data to determine causal relationships under certain conditions. Previously, the main reason observational data could not be used to determine causal relationships was due to statistical confounding whereby multiple effects (possibly containing causal or merely correlated effects) were mixed together. When confounded, these effects can neither be distinguished nor separated from each other. Hence the term, "confounded." One of Pearl's main technical achievements is the development of the do-calculus, where causal effects can be determined from observational data in most situations under mild conditions.[3] Example questions that can be answered at this rung of the ladder include: "If I take aspirin $\mathbf{(do(}x\mathbf{))}$, will my headache go away (y)?" or "What would happen to the cancer rate (y) if smoking were banned $\mathbf{(do(}x\mathbf{))}$?"

The third and final rung of the ladder is *Counterfactuals*, which corresponds to the human activity of imagining or retrospection. On this rung, the experimenter can reason about the probability something would happen contrary to what actually occurred. Mathematically this is written as $P(y_x|x')$. "Would my headache have gone away (y_x), if I hadn't taken (x') that aspirin (x)?" or "What would the world be like (y_x) if gravity were different (x') than it is (x)?" are examples of the types of questions that can be asked at this level.

Causal reasoning is the distinguishing characteristic of human reasoning and inquiry. Many contend with Pearl that human-like reasoning in machines cannot be realized unless machines are able to operate at all three rungs of the Ladder of Causation.[4]

Causal Models

Figure 4, below, is an example of a simple causal model represented by a causal diagram. A causal diagram is nothing more than a directed acyclic graph (DAG) where the nodes are measurable outputs (i.e., variables) of a system and the directed edges indicate a causal relationship between them. Informally, the directed edges can be thought of using the metaphor "listens to." The directed edge from A to B indicates that B listens to A when determining its output value. Similarly, nodes C and D listen to B to set their output value, while E listens to both C and D.

The absence of an arrow is equally important as this indicates who a node does *not* "listen to." Thus, in Figure 4 the one edge from A to B asserts that Node B listens to A *and only* A in determining its output value. Thus, DAG models the invariant causal relationships that are either known or assumed for a given process or system. If the functional relationship between the nodes is known, this can be included in the causal analysis. The formal abstract model of Figure 4 is:

$A=f_A(U_A)$, $B=f_B(A, U_B)$,
$C=f(B,U_C)$, $D=fD(B, U_D)$, and
$E=f_E(C,D,U_E)$

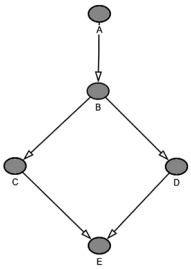


Figure 4: Causal Diagram of a Simple System[4]

where Ux is some unmeasured or unmeasurable latent variable (e.g., noise), and fx is a function that defines precisely how the node determines its output value. This function, fx, can be linear or non-linear, continuous, or discrete, parametric or non-parametric.

Even without knowledge of the actual functional relationships between nodes, the representation of who listens to whom shown in a simple DAG provides a significant amount of structural information. First, it makes explicit the known or assumed causal relationships within the system. Thus, the DAG forces an analyst to show their hand, thereby openly declaring assumptions and/or presenting their knowledge about how a system operates. Second, if the DAG accurately captures the actual causal relationships in a system, certain statistical relationships or testable implications will be reflected in the data. For example, if Figure 4 reflects the actual causal relationships of a given system then particular conditional independencies between nodes will be reflected in data collected from the system. These can be easily checked using virtually any statistical software package. In Figure 4 the following conditional independencies (i.e., $\perp$) must hold: $B \perp E \mid C, D$; $A \perp E \mid C, D$; $A \perp E \mid B$; $A \perp C \mid B$; $A \perp D \mid B$; and $C \perp D \mid B$.

Consider the first conditional independence, $B \perp E \mid C, D$. This asserts that given the values C and D are held constant, say via intervention, the variables B and E will exhibit statistical

independence. If these conditional independencies do not hold, then the data and the DAG are incompatible. What follows from this is, even when the testable implications hold, that does not constitute a proof that the specified causal model is correct, but rather indicates that the specified model is not incorrect. This is akin to statisticians declaring that two systems are statistically not different. One cannot properly declare two different random variables the same because the observation period is necessarily finite. This means there may be several causal models compatible with the data. This should not be seen as a negative as it provides a ready basis for reasoning about plausible explanations for what has been observed.

Take as a concrete example the previously presented data from Table 2 and the causal diagram from Figure 4. Since edges represent causal relationships, the question that could not be answered before from the data alone, namely, does A *cause* E can now be answered affirmitively. A does cause E because E listens to D, D listens to B, and B listens to A—a chain of causality.

The causal diagram of Figure 4 is actually a causal diagram of a firing squad.[4] As shown in Figure 5, Node A represents the court which, when it takes on the value of 1, has issued an execution warrant. Node B is the Commander who without fail issues the order to fire (i.e., 1) upon receiving a warrant. The riflemen (Nodes C and D) are expert marksmen who always fire when ordered to do so by their Commander (i.e., 1) and always hit their target. Node E is the victim who dies (i.e., 1) whenever either (or both) C and D fire. The triangular symbol in Node A indicates it is the exposure variable while the "I" in Node E indicates it is the outcome variable. This graphically depicts the question, "Does A cause E?" or, "Is the Court issuing the warrant causally related to the death of the victim?" Of course, the answer is yes. But this was impossible to ascertain from the data in Table 2 without knowing the data generating process (i.e., $\boldsymbol{M}$).

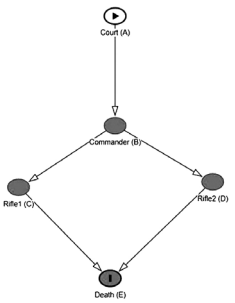


Figure 5: Causal Diagram of a Firing Squad[4]

The data in Table 2 reflects the firing squad operating as intended. However, now that the data generating process $\boldsymbol{M}$ is known, questions from rungs higher in the Ladder of Causation can be answered that before could not be determined using only the data collected from the system. For example, it was previously determined that A causes E. But what would the value of E be if, due to an intervention, C was set to 1? This situation is reflected in Figure 6. Note that C no longer listens to B; the arrow has been removed. The question being asked is essentially: What is the value of E if C is 1, independent of A, B, and D? The answer is, no matter what the

other node values are, E will be 1. The rifleman is an expert and never misses. We can conclude this outcome even though the following combination of node values has not been observed (i.e., A-E being 0 0 1 0 1, respectively). In fact, if X represents "don't care" it can be concluded that if C = 1, E = 1 in a total of 7 situations that have not been observed (i.e., A-E being X X 1 X 1, respectively).

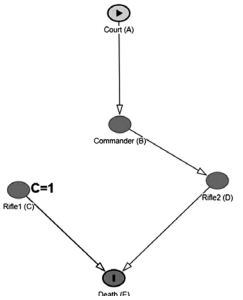


Figure 6: Firing Squad Intervention[4]

Moving to the final rung of the ladder, Counterfactuals, one can use ***M*** to analyze the situation where the firing squad operated as intended (i.e., A-E was 1 1 1 1 1, respectively) and imagine whether the outcome, E, would have been different if C had been 0 (i.e., A-E was 1 1 0 1, respectively). Given the causal model, ***M***, the answer is the outcome would have been the same. Node E would still be 1.

That this is completely obvious and even trivial is the fact that proves the point. For it is manifestly NOT obvious or trivial to a machine or algorithm that only has access to the data in Table 2. Furthermore, no amount of additional data (from a correctly operating system) would have helped. With a causal model though, reasoning about interventions and counterfactuals is readily accomplished.

An additional benefit of causal models in the form of DAGs is the ability to discover analogous situations across disparate domains. This situation is depicted in Figure 7, below. The causal model for the firing squad in the left-most section of the figure is from the legal/law enforcement domain but it describes a similar system from the aerospace domain in the middle of the figure. The aerospace system is a landing gear deployment system where an Aircraft Commander (A) initiates landing gear deployment by authorizing the uplock hook command via a relay (B) which signals two hydralic actuators (C and D) to lower the landing gear (E). Even more generally, the analogy extends to a dual-redundant command and control system from the even broader domain of system reliability as shown in the right-most causal model of Figure 7. Thus, this demonstrates how a system that works in one domain can potentially (and perhaps drastically) reduce the learning curve required to understand systems in a related domain. Given the readily available algorithms to quantify graph similarity, the DAG becomes an even more attractive representation of causality.

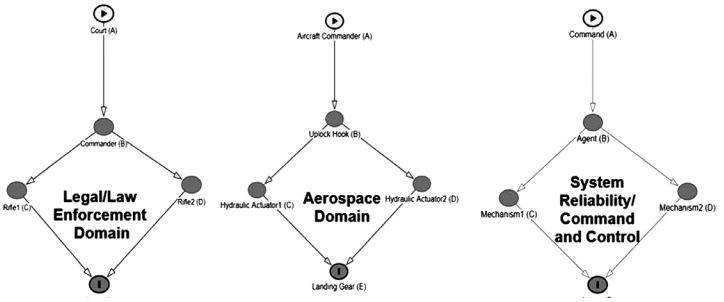


Figure 7: Analogies from Causal Models

Causal Reasoning in a Sports Medicine Scenario

A more complex and realistic example[5] comes from the field of epidemiology.[6][10] The causal model in Figure 8, below reflects a research team's consensus on causal factors related to participant injuries during a sports game. It is not directly based on data, but rather on their collective experience. The question considered is: Are Warm-Up Exercises (WUE) a causal factor of Injury (I)? and, is indicated by the light-gray arrows. Data for each one of these variables was collected and the testable implications were analyzed to verify compatibility between the data and the causal model using the statistical software, R, with the package daggity. Figure 9, below, shows the R program. In this case, analysis revealed the causal model and the data were indeed compatible; all required conditional independencies were reflected in the data.

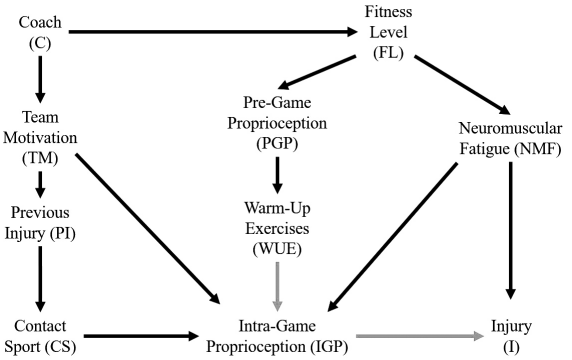


Figure 8: Sports Injury Causal Model

```
# load the R package `dagitty`
library(dagitty)
# load data from a text file
d <- read.csv("http://dagitty.net/sports.csv")
# download DAG from dagitty.net
g <- downloadGraph("dagitty.net/mN4IKjR")
# evaluate the d-separation implications of the DAG
r <- localTests(g, d)
# perform Holm-Bonferroni correction
r$p.value <- p.adjust(r$p.value)
# focus on tests with p-values below a threshold
r <- r[r$p.value<0.05,]
# plot results
plotLocalTestResults(r)
```

Figure 9: R "testable implications" Program[5]

Suppose, however, that the causal model was not specified correctly; suppose a causal relationship was inadvertantly omitted. This is the case in Figure 10 where the directed edge between Team Motivation (TM) and Warm-Up Exercises (WUE) has been removed. Now the resulting output from the R program of Figure 9 shown in Table 3 below indicates that in three instances the conditional independencies of the listed variables did not hold. Namely, Team Motivation (TM) should be conditionally independent of Warm-Up Exercises (WUE) given Pre-Game Proprioception (PGP), Fitness Level (FL), and Coach (C), respectively. However, the *p*-values (i.e., the values in the p.value column of Table 3) did not exceed the required threshold of 0.05 and therefore this is not the case.[1] Thus, an error in the causal model or, equivalently, a misunderstanding of causal relationships in the situation under consideration can be detected objectively and explicitly.

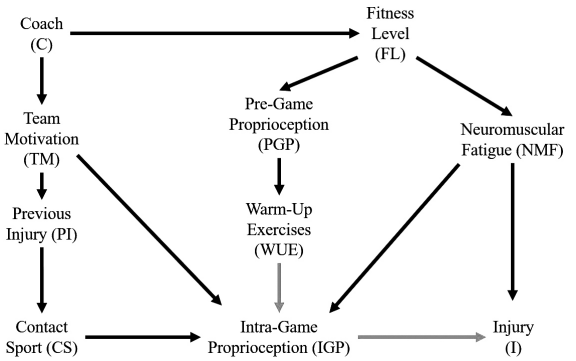


Figure 10: Sports Injury Causal Model with TM/WUE Edge Removed[5]

Table 3: R Output from "testable implications" Program

	estimate	std.error	p.value	2.5%	97.5%
TM _||_ WUE | PGP	0.2463031	0.04241572	7.273348e-07	0.1629669	0.3296393
TM _||_ WUE | FL	0.2397066	0.04189577	1.150645e-06	0.1573919	0.3220212
TM _||_ WUE | C	0.2287258	0.04109466	2.649499e-06	0.1479851	0.3094664

As a final result, estimates of the path coefficients can be determined from the causal model and the data.[2] That is, a numerical estimate of the causal effect of WUE on I can be determined. Figure 11 shows the simple R program used to calculate the coefficients, Figure 12 shows the resulting output which includes various summaries of fit indices on the left (i.e., quality metrics for the path coefficient estimates) as well as path coefficient estimates themselves on the right. The causal diagram with the path coefficients annotated is shown, below, in Figure 13.

1 The null hypothesis is that the tested variables are conditionally independent (i.e., using causal terminology, *d*-separated). Since the *p*-values are less than the specified threshold of 0.05 the null hypothesis is rejected: the variables are *not* conditionally independent.

2 Data has been scaled and normalized.

```
library(dagitty)
library(lavaan)
#load data from a text file
d <- read.csv("http://dagitty.net/sports.csv")
# CORRECTED DAG
g <- dagitty('dag {
+ C [pos="-4.000,-3.000"]
+ CS [pos="-4.000,3.000"]
+ FL [pos="1.000,-3.000"]
...
# Convert to lavaan object, fit model to data,
# Determine and display path coefficients
m=toString(g, "lavaan")
fit=sem(m, d)
summary(fit)
```

Figure 11: R Program to Calculate Path Coefficients[5]

```
lavaan 0.6-3 ended normally after 14 iterations

  Optimization method                           NLMINB
  Number of free parameters                         23

  Number of observations                           500

  Estimator                                         ML
  Model Fit Test Statistic                      22.771
  Degrees of freedom                                29
  P-value (Chi-square)                           0.787

Model test baseline model:

  Minimum Function Test Statistic              612.933
  Degrees of freedom                                44
  P-value                                        0.000

User model versus baseline model:

  Comparative Fit Index (CFI)                    1.000
  Tucker-Lewis Index (TLI)                       1.017

Loglikelihood and Information Criteria:

  Loglikelihood user model (H0)              -5370.189
  Loglikelihood unrestricted model (H1)      -5358.803

  Number of free parameters                         23
  Akaike (AIC)                               10786.378
  Bayesian (BIC)                             10883.314
  Sample-size adjusted Bayesian (BIC)        10810.311

Root Mean Square Error of Approximation:

  RMSEA                                          0.000
  90 Percent Confidence Interval          0.000  0.023
  P-value RMSEA <= 0.05                          1.000

Standardized Root Mean Square Residual:

  SRMR                                           0.026
```

```
Parameter Estimates:

  Information                                 Expected
  Information saturated (h1) model          Structured
  Standard Errors                             Standard
```

Regressions:

	Estimate	Std.Err	z-value	P(>|z|)
FL ~				
C	0.242	0.041	5.857	0.000
TM ~				
C	0.189	0.043	4.378	0.000
IGP ~				
CS	0.314	0.036	8.742	0.000
PI ~				
CS	0.302	0.043	7.027	0.000
NMF ~				
FL	0.346	0.045	7.739	0.000
PGP ~				
FL	0.317	0.046	6.960	0.000
I ~				
IGP	0.307	0.040	7.599	0.000
NMF	0.256	0.040	6.463	0.000
IGP ~				
NMF	0.219	0.036	6.061	0.000
WUE ~				
PGP	0.184	0.043	4.320	0.000
IGP ~				
TM	0.233	0.038	6.073	0.000
PI ~				
TM	0.306	0.044	6.892	0.000
WUE ~				
TM	0.258	0.044	5.824	0.000
IGP ~				
WUE	0.272	0.037	7.371	0.000

Figure 12: R Path Coefficients Program Output

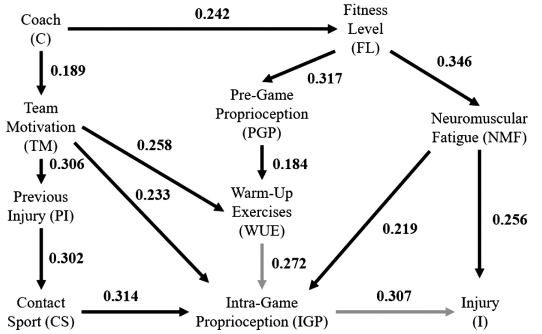


Figure 13: Sports Injury Causal Model with Path Coefficients

Using the path coefficients, the causal effect is easily determined. The effect of WUE on I, i.e., $f(WUE, IGP)$, is simply the product of the path coefficients on the light-gray causal path between WUE and I. That is $I = f(WUE, IGP) = 0.272 \cdot 0.307\ WUE = 0.0835\ WUE$. The significance

of achieving a causal result, to say nothing of a numerical causal result, from observational data is considered astounding and even unbelievable or impossible by many statisticians. Nevertheless, this type of analysis is routine in the fields of biology, medicine, and social sciences and has been for decades.[4] [5] [6] [7]

Autonomous Systems and Intelligent Machine Applications

There are several fundamental areas where causal analysis can be used to advance AS and IM cognitive capabilities. Fortunately, much of the software needed to perform the critical manipulation, analysis, and testing of causal models and other data structures has already been implemented in statistical packages like daggity and lavaan from the R statistical software suite and are available via Application Programming Interface (API) calls from any number of languages. They are also readily available in equivalent statistical and structural equation modeling software suites. Thus, the required foundational computational and statistical tools are in place, mature, and ready to be used in the development of the capabilities described below. Some ideas of AS and IM applications include the following:

- ***Knowledge Storage and Retrieval***

  This capability is fundamental to many, if not most, areas within AS and IM. Since the DAG serves as the core data structure for causal information and stores fundamental causal knowledge, the rich set of graph theory algorithms to analyze and characterize DAGs can be brought to bear. Furthermore, graphs, especially sparse graphs, can be very efficiently stored, retrieved, and compared. Some knowledge storage and retrieval capabilities include the following:

  - Searching for similar causal models or those models similar (as measured by graph similarity metrics) to the situation reflected in the observed (and possibly real-time) data.
  - This capability can additionally serve as a basis for discovering analogies by analyzing/comparing causal models that meet some minimum similarity threshold.

- ***Learning***

  - Given two approaches to accomplish a task, evaluate multiple virtual "what if" scenarios to discover a more efficient or effective approach (i.e., different causal paths that achieve the same effect). Routines to simulate the operation of a causal model are readily available, relatively efficient, and fast.

- ***Discovery***

  - Build causal model(s) of the operating environment via observations alone. Employ human experts to refine the models with feedback from the AS/IM as to whether the suggested refinements are compatible with the observed data.

- Similarly, develop an IM to observe the environment via sensors/other instruments and propose causal explanations for the collected data. That is, the IM will provide plausible explanations via causal diagrams that are readily interpretable by humans.

- ***Explainable AI***
  - Given causal diagrams annotated with path coefficients that represent metrics such as cost or efficiency, an IM or AS can explain why it recommends a course of action (COA) X over Y, "It was more efficient than any alternative. Shall I list the other COAs I considered and explain why I didn't choose them?"
  - By treating a causal diagram as a road map, existing routing and mapping algorithms and optimization routines can be brought to bear. Given a causal diagram annotated with an AS's or IM's ability to influence certain causal outcomes and the cost to do so (both of which may vary over time), the AS/IM can readily explain why a task was done the way it was at that particular time, "I would have accomplished the task in the preferred way, but at the time, my ability to modify this system parameter was disabled/malfunctioning."
- ***Experiments without (more) data***
  - The question, "what would happen if I did this?" can be investigated by direct manipulation (i.e., intervention) of the causal model.
  - The question, "what would happen if I had done this instead?" can be explored using the causal model to imagine alternative outcomes.
  - The resulting causal models can be compared to the current/actual model of reality to evaluate alternative COAs.
- ***Policy evaluation***
  - The question of whether a person/organization/system is conforming to a given policy can be determined by comparing the policy (i.e., a causal model of how the world "should" be) to data from the real world. If the causal model and the data are compatible, this indicates the specified policy is being followed.
  - If they are incompatible, alternative models that are compatible with the data can be generated and compared to the should-be model to identify the possible areas of non-compliance.

There are many other potential AS/IM applications, but those identified above serve to demonstrate the rich and diverse areas in which causal reasoning is both applicable and can bring unique capabilities to AS's and IM's.

Causal Reasoning Framework (CRF)

The Causal Reasoning Framework (CRF), as shown in Figure 14, organizes the foundational components needed for causal inference and reasoning into a unified whole. The CRF is intended to be the basis for further experimentation and research into causal analysis and inference. To provide maximum flexibility, CRF was developed using open source, royalty-free components. The two main components of CRF are Soar[11] and R.[12] Soar will be explained in more detail below.

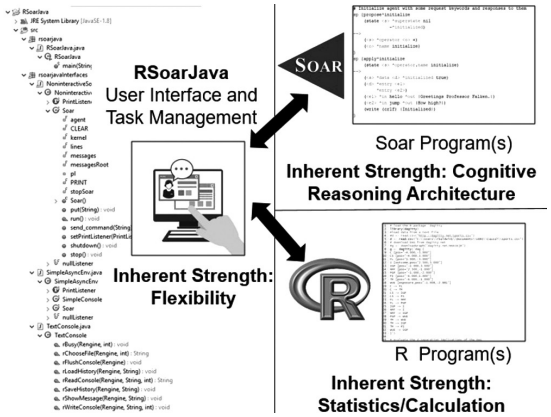


Figure 14: The Causal Reasoning Framework (CRF)

Briefly, however, Soar is an open-source cognitive architecture whose functional capabilities and architectural elements mimic the principle areas used in human cognition. Soar has been in development for over 35 years, is well-documented, and provides robust and stable computational building blocks for CRF. The inherent strength of Soar is its cognitive reasoning architecture.

R is a programming language and software environment for statistical computing. It is widely used in the area of AI, ML, causal analysis, and of course, statistics. It has a large and active user base and a core set of packages with over 15,000 additional packages available. It is supported on Windows, Linux, MacOS, and other platforms. R serves as the computational platform for Soar. The inherent strength of R is its rich statistical capabilities and robust API.

The final component of CRF is RSoarJava, which is a Java-based, "wrapper" application that is intended to provide user interface and task management functionality. It currently has a rudimentary capability to exchange data with both Soar and R via their respective APIs. RSoarJava's inherent strength is flexibility.

Soar, the cognitive architecture for CRF, is ideally suited for causal reasoning and analysis in that Soar presumes some initial state and a desired state and then applies operators to move towards the desired state. The Soar architecture includes the general capabilities and logic for automated decision-making, multiple types of learning, problem solving, and hierarchical

planning. This greatly reduces the technical risk as development efforts can be directed to formulating the Soar rules, productions, and other procedures to develop causal applications rather than developing and debugging fundamental cognitive memories, capabilities, and learning mechanisms.

Figure 15 below shows the major architectural elements of Soar. Working Memory is a shared short-term representation of the current situation represented by a single, connected, directed graph. Production Memory stores knowledge about how to do things (e.g., procedures). Semantic Memory contains long-term contextual knowledge about objects or concepts as represented by disconnected graphs consisting of multiple directed sub-graphs. Episodic Memory captures temporally ordered information along with the context of when and how an episode was experienced. Reinforcement Learning (RL) can be used to guide operator selection based on a reward function, chunking captures general knowledge gained from impasse resolution. Semantic and episodic learning derives knowledge based on past experience. Functionally, the knowledge contained in Soar episodic and semantic memory is stored in a memory-based SQLite database. Soar supports all major platforms, is open source and has a domain independent API. It has bindings to many languages including C/C++, Java, Python, and TCL.

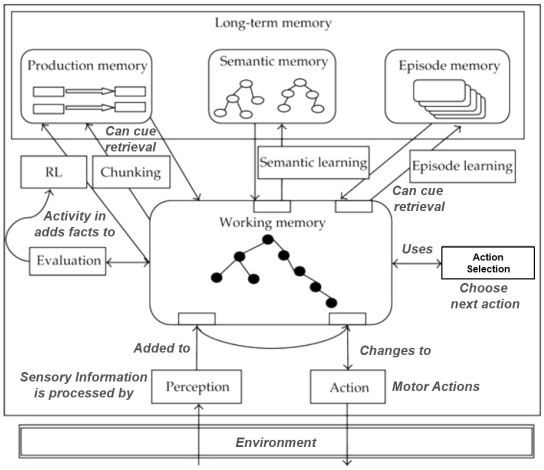


Figure 15: The Soar Cognitive Architecture[11]

In Figure 16 below, the CRF inference engine is shown. It has been adopted wholesale from Pearl's inference engine[13] and serves as the paradigm for CRF component interaction as well as for the presumed workflow resulting from a causal query, which the following description is based on.[13] The engine accepts three inputs and produces three outputs. The directed arrows in the figure indicate information flow between inference engine components. The icons in the blocks of the inference engine indicate the CRF component providing that functional capability. On the input side, the Query is presumed to be supplied by a CRF user via RSoarJava, while initial causal model(s) (i.e., Assumptions) and the Data is provided via domain experts and the

domain, respectively. On the output side, Soar takes as input the causal model(s) and the query and formulates the "Estimand," $\boldsymbol{E_S}$. That is, the schema or recipe for answering the query. The Estimand, $\boldsymbol{E_S}$ and the data is used by R to calculate an Estimate or answer to the query, $\hat{\boldsymbol{E}}_S$. Fit Indices, $\boldsymbol{F}$, measure how well $\hat{\boldsymbol{E}}_S$ answers the query and is produced by R. As can be seen in the figure, these results are provided to Soar. As conceived below, Soar provides the heavy lifting with respect to acting on the causal inferences made by the inference engine to accomplish any tasks associated with the AS/IM applications.

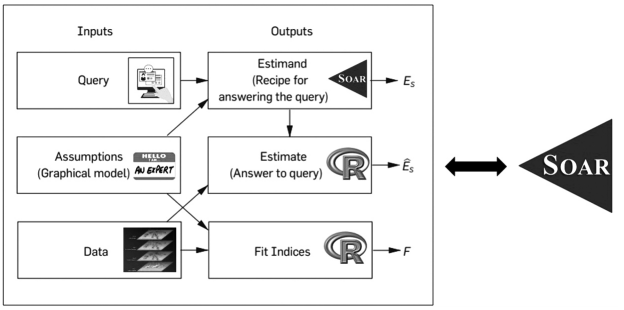


Figure 16: CRF Inference Engine based on[13]

Using Pearl's inference engine design as adopted and incorporated into the CRF, the "7 tools of Causal Inference"[13] can be realized and used to power new and unique applications for AS and IM. These tools include the following:[13]

1. Transparency and testability via encoding causal assumptions
2. Intervention and control of confounding via do-calculus
3. Answer "what if" questions via developing algorithimitization of counterfactuals,
4. Assess direct and indirect effects via causal mediation analysis
5. Robustness (i.e., adaptability, external validity, overcoming sample selection bias) via do-calculus
6. Recovery from missing data via assessing causal model(s) of the "missingness" process
7. Causal discovery via evaluation of models compatible with collected data.

Cyber Defense Strategy Observations

An increasing number of industry insiders believe more creative thinking, more research, more knowledge management and more causal reasoning with autonomous systems and intelligent machine applications—not just more technology—is needed. Dr. Thomas Homer-Dixon outlined this ingenuity gap, "in general, as the human-made and natural systems we depend upon become more complex, and as our demands on them increase, the institutions and technologies we use to manage them must become more complex too, which further boosts our

need for ingenuity. The crush of information in our everyday lives is shortening our attention span, limiting the time we have to reflect."[14] It is these increasing demands, combined with today's greater network complexity, and rising social unpredictability, that make it more critical than ever that smart technical and social solutions be ready at a moment's notice. The MIT scientist Edward Lorenz's Chaos Theory is also used to describe how small changes can lead to widely varying results and path dependence.[15] As such, it is essential to leverage a new cyber situational awareness (SA) model that incorporates the aforementioned: causal reasoning with autonomous systems and intelligent machine applications.

Protecting enterprise networks and providing mission assurance without significant autonomous systems supporting cyber-SA and warning capabilities will continue to be a challenging mission. Without causal reasoning with autonomous systems, we are left with a fragmented, imperfect view into enterprise networks and how cyber assets map to tasks, objectives, and missions. This incomplete view thwarts threat detection, trend analysis, and preemptive actions which fosters slow or non-existent reactions to threats and changing conditions. An environment like this constricts a senior leader's decision-making space. Cyber-SA for most enterprises is presently disjointed, rudimentary, ad hoc, too focused on technical analysis, lacking important cyber threat intelligence data feeds from supporting providers, and missing actionable, contextual analytics provided by causal reasoning within autonomous systems. Moreover, personnel are currently delivering very limited strategic cyber-SA capabilities for senior leadership.

This flawed view can be operationally blinding to any organization. Initial progress has been made today by many organizations to increase their causal reasoning with autonomous systems capabilities to enhance their organizational cyber-SA capabilities, for example, security operations centers with advanced networks and AI algorithms. However, many organizations may further strengthen their cyber-SA and warning capabilities by weaving an empowered cyber-AI construct with causal reasoning attributes into their enabled mission assurance strategy. This construct has a high return on investment for any organization operating in today's high threat environment.

The time has arrived for a new model, more ingenuity, and the recognition of the importance of cyber-SA in defense of an organization's enterprise. What matters in transforming an organization's cyber–SA is causal reasoning with autonomous systems that increase intelligence, integration, speed, analytics, expertise, and resiliency. Enacting just such a cyber-AI causal reasoning with autonomous systems framework can and will enable an organization to more effectively protect itself today and in the future.

CONCLUSION

Causal analysis is essential for realizing the vision of human-like reasoning: it brings the ability to determine cause-effect relationships and provides a basis for reasoning about interventions (i.e., doing), as well as what might have happened had events occurred differently (i.e., imagining/retrospection) which are fundamental characteristics of human reasoning. Causal analysis has seen widespread use and success in epidemiology, social science, and other fields for decades. Even so, its use in engineering, computer science, and AI, has been limited and its potential is just beginning to be widely recognized and applied. For all the progress that has been made in the field of AI, machines with human-like intelligence are still not a reality. Like the story of Theseus and Dr. Shannon's electromechanical mouse, there is promise for those in the field of AI to find a path through the maze as well.

NOTES

1. Daniel Klein, "Mighty Mouse," MIT Technology Review, 2018, 1.
2. Robert Schalkoff, *Intelligent Systems: Principles, Paradigms, and Pragmatics*, Jones & Bartlett, 2011, 14.
3. Judea Pearl, *Causality (2nd Edition): Models, Reasoning, and Inference*, Cambridge University Press, 2009.
4. Judea Pearl, *The Book of Why: The New Science of Cause and Effect*, Basic Books, 2018.
5. Johannes Textor, et al., "Robust causal inference using directed acyclic graphs: the R package 'dagitty,'" *International Journal of Epidemiology*, 45:6, 2016, 1887-1894.
6. Mikel Aickin, *Causal Analysis in Biomedicine and Epidemiology*, Marcel Dekker, Inc., 2002.
7. Rex Kline, *Principles and Practice of Structural Equation Modeling*, Guilford, 4th Edition, 2016.
8. Fangzhen Lin, "Embracing Causality in Specifying the Indirect Effects of Actions," *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, Quebec, Canada, August 1995, 1985-1991.
9. Judea Pearl, *The Mathematics of Cause and Effect: With Reflections on Machine Learning,* Microsoft Research, Video Presentation.
10. Bill Shipley, *Cause and Correlation in Biology 2nd Edition*, Cambridge University Press, 2016.
11. John Laird, *The SOAR Cognitive Architecture,* MIT Press, 2012.
12. R Core Team, *An Introduction to R*, available on-line at https://cran.r-project.org/ doc/manuals/r-release/R-intro.html, Version 3.6.2, 12 Dec 19.
13. Judea Pearl, "The Seven Tools of Causal Inference, with Reflections on Machine Learning," Communications of the ACM, March 2019, 54-60.
14. Homer Dixon, "How Can We solve the Problems of the Future?" The Ingenuity Gap, Knopf Publishing, 2000, 4.
15. Edward Lorenz, *Predictability: Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas?* Retrieved from https://mathsciencehistory.com/wp-content/uploads/2020/03/132_kap6_lorenz_artikel_the_butterfly_effect.pdf , 1972.

DoD Has Over 3.5 Million Insiders – Now What?

A User Online Risk Score Framework To Reduce The Insider Threat

Lieutenant Colonel (P) Stephen A. Roberts, Ph.D.

ABSTRACT

DoD employs about 3.5 million military and civilian direct employees, contractors, and reserve personnel. In addition, over 50,000 contracted entities (e.g., groups and organizations) can connect directly to the DoD Information Network (DoDIN) to collaborate and protect DoD systems and sensitive data. These imperfect users often interact with DoD across multiple classification domains and IT systems. Without focusing on potentially damaging insider activity, DoD will fail to meet the 2018 Cyber Strategy objectives, and adversaries will continue to erode our technical overmatch while imposing excessive remediation costs. This erosion occurs not only through attacks using technical means but also through exploitation of insiders. This article will introduce and urge the implementation of a framework to more effectively address insider threats by providing an empirical measure of each user's risk through their actual behaviors. This model will give the user near-real-time awareness of personal behaviors counter to organizational policy and cybersecurity requirements. This measure will also empower management to target training, remediation, and risk reduction while also allowing decision-makers to determine which user risk-exposed areas, roles, or practices require additional remediation. As a result, all organizational decision levels will be better able to improve cybersecurity resiliency in the face of an ever-evolving insider threat landscape.

INTRODUCTION

To fully achieve the latest Cyber Strategy (2018) goals, DoD must effectively implement a comprehensive insider threat program. The National Insider Threat Policy and Minimal Standards for Executive Branch Insider Threat Programs (EO 13587) and DODD 5205.16 outline requirements for an insider threat program (2012

Lieutenant Colonel (P) Stephen A. Roberts, Ph.D., a 30-year DoD veteran, is a Cyber Branch Officer now serving as the ARCYBER G30 LNO at Fort Meade, MD, and previously served a yearlong Senior Service College Cyber fellowship at Carnegie Mellon University. He holds a Bachelor of Science in Computer Information Systems, three Masters of Science (Computer Science, Computer Forensics, and Government Information Leadership with emphasis on Cybersecurity), and a Ph.D. in Cybersecurity with an emphasis on Insider Threat. He holds certifications as a Federal Chief Information Officer (CIO), Federal Chief Information Security Officer (CISO), CNSS/NSTISSI 4011, 4012, 4015, 4016, Security Plus, and CISSP.

and 2014 respectively),[1] which cover user awareness training along with monitoring and detection of malicious insiders, but make no mention of non-malicious insider activity. Today, years after these standards were first codified, a 2018 DoD Inspector General (IG) report confirms non-compliance with these minimal policy standards.[2]

Without focusing on potentially damaging insider activity, DoD will fail to meet the 2018 Cyber Strategy objectives.[3] More importantly, adversaries will continue to erode our technical overmatch and impose excessive remediation costs. This erosion occurs through attacks using technical means as well as by exploiting malicious and non-malicious insiders.[4] This article urges the immediate implementation of an empirical user behavior measurement framework to drive individual awareness, compliance, and accountability, which will reduce an adversary's ability to conduct daily operations and enable management to more effectively address the insider threat. It will also allow senior leaders to see organizational cybersecurity strengths and weaknesses at the user level, allowing the empirical decision support that is lacking today.

Malicious Insiders

Malicious insiders are organizational users with access and hence have a unique ability to exploit information technology (IT) assets to harm the organization, its customers, or its employees.[5] While representing a tiny percentage of the workforce, these insiders often plan and execute attacks over long periods of employment,[6] and their impact can psychologically devastate entire organizations. In addition, these trusted actors interact personally with colleagues as team members and, with no warning, betray organizations with a level of deceit that devastates colleagues and organizational cultures for long periods.[7] The US has suffered its share of significant malicious insider incidents, such as Private Manning, Edward Snowden, and Robert Hanssen.[8]

The impact of each successive compromise increases as the data accessible within IT systems also expands. These losses have led to reactionary and wholly inadequate policy changes to prevent compromise recurrence.[9] The apparent daily loss of personal information and intellectual property compounds injury caused by these malicious insider events. Collectively, insider-attributed losses continually add to what has been identified as the most significant transfer of wealth and knowledge in human existence.[10] Moreover, these compromises are not only attributable to the malicious insider but also the non-malicious insider.

Non-Malicious Insiders

DoD must continue to pursue programs to identify and manage the unique malicious insider threat. Still, non-malicious insiders can also have devastating, long term impacts, given their ongoing, sometimes multi-year interaction and decision-making related to DoD IT systems.[11] Non-malicious insiders typically make a myriad of poor decisions (e.g., by clicking on spam email links, misplacing Common Access Cards [CAC], leaving devices unlocked, visiting insecure websites, introducing malware onto networks, leaving government assets unsecured, or ferrying DoD data across home and public resources). These imprudent actions are often due to ignorance, impatience, gullibility, or the promise of a short-term increase in productivity.[12] The DoD employs about 3.5 million military and civilian direct employees, contractors, and reserve personnel.[13] In addition, over 50,000 contracted entities (e.g., groups and organizations) can connect to the DoD Information Network (DoDIN) to collaborate and protect DoD systems and sensitive data.[14] These imperfect human users often interact with the DoD across multiple classification domains and IT systems.[15] To illustrate the problem, if only 0.1% of the insiders produce one activity per year resulting in an incident, this equates to more than 3,500 annual incidents even if the impact of the contracted entity workforce is ignored.

Many of the same insider threats that plague the DoD also plague large commercial entities. For example, 85% of commercial sector data breaches involve human error. More troubling, the average time to detect a violation exceeds 220 days, and the time to correct an incident is an additional 80 days.[16] Meanwhile, the DoD also faces multiple, dedicated, nation-state-sponsored adversaries and advanced persistent threats (APT).[17] The adversarial threats patiently find and exploit the weakest link, which far too often is the insider.

A complete cybersecurity strategy includes technical, procedural, and physical controls.[18] DoD has implemented a complex cybersecurity model that implements a significant IT and technical security controls investment to combat global risks. The 2018 Cyber Strategy mentions many of these technical controls. Still, it seriously neglects the insider threat and the tools and awareness that senior leaders and managers need in order to identify or mitigate these issues. Generalized annual user awareness training is often the only tool leadership is provided with, which only marginally addresses the risk. In addition, security best practices prescribe an architecture with several layers of complementary defensive capabilities, commonly referred to as a Defense-in-Depth.[19] For example, a primary component of DoD's

technology investment is the Joint Information Environment (JIE), representing $1 billion of its overall $42 billion annual IT investment.[20] Yet, despite this significant technological investment, either malicious or non-malicious insider actions can quickly defeat the effectiveness of these expensive technical controls.[21]

The DoD workforce provides the muscle, ingenuity, and productivity critical to mission accomplishment. It is also made up of imperfect humans. Research overwhelmingly confirms that humans are poor decision-makers regarding cyber risk evaluation and cybersecurity policy compliance.[22] Mere chance often prevents poor risk decisions from resulting in catastrophic compromise. Absent constant monitoring and behavior re-emphasis, poor behavior will remain a given. Lack of immediate adverse consequences leads to a new normal of self-serving or complacent behaviors until a costly cyber incident occurs at the hands of an opportunistic and patient adversary. Management and users typically do not acknowledge a problem until the breach is discovered, and the forensics, if conducted, uncovers the causative user activity. Often, these results may not be available for months or even years after the attack event.

Considerable research has sought to determine the reasons, behaviors, or triggers that cause woeful compliance by well-meaning users.[23] However, from a risk perspective, more important than the why of human behavior, is the existence and scale of this risk. Insider threat controls must manage this risk more completely. These controls must enable empirical management visibility, drive personal awareness and accountability, and target training that improves compliance and overall cybersecurity risk.[24] The DoD cannot leave cybersecurity at the user level to chance, given the stakes posed by near-peer adversaries with collectively greater resources, patience in achieving effects, and aggressive cyber exploitation policies.[25]

Recommended Strategy

Information Assurance (IA) training has been used to improve user cyber risk perception and decision making. The DoD has implemented mandatory annual training, but achieving 100% compliance has proven difficult, thus limiting the collective benefit. Research indicates that static training approaches, similar to those implemented by DoD, are ineffective.[26] Fear, punishment, and peer pressure mitigation approaches are equally weak.[27] Instead, mixing targeted training to raise specific user awareness and increased personal responsibility has proven more effective.[28] DoD should adopt these more dynamic approaches to optimize training efficiency better. Following an initial focus on base cybersecurity policies, individually measured risk behaviors that cover user gaps would overall raise the workforce's cyber efficacy and improve DoD's overall cybersecurity posture.

Using the Fair Isaac Corporation (FICO) credit score and creditworthiness model may be instructive for the next component of the recommended strategy. Used by the industry as an indicator of creditworthiness, a FICO score measures a person's credit trustworthiness based on historical financial behaviors and demographics.[29] Users can actively monitor their credit scores in many ways,[30] and this awareness significantly improves credit behaviors, knowledge,

and average FICO scores.[31] FICO scores assist credit providers in making monetary trust decisions that will impact the provider and financial community of lenders and consumers alike. Monitoring applications allow users to see real-time changes in scores and provide training and guidance on improving scores.[32] Despite a lack of formal financial training, FICO monitoring educates and perceptibly alters behaviors that benefit the community and the user.[33] For the DoD, user cybersecurity monitoring would similarly provide a user-specific score by calculating compliance using various key measurement factors (e.g., Internet search patterns, email patterns, cyber policy adherence). This "online risk score" feedback can appear on the user's desktop screen to enable direct feedback and tailored training and instruction for specific behavioral challenges. Focused education would reduce non-compliance and stimulate positive score results, thus emphasizing healthier organizational cybersecurity behaviors.

This online risk score over time would be affected by a user's specific behaviors. Scores would be aggregated at several decision-making levels: individual, supervisory, departmental, and organizational, making users accountable for compliance behaviors and improving remediation visibility throughout the decision chain. Measuring personal and corporate accountability allows targeted management, mitigation, investment, and training at crucial risk sites and enables positive incentives and recognition for compliant behaviors. Scoring should be tailored over time to meet the changing threat landscape. Factors to track behaviors and their periodicity can reflect compliance trends (e.g., malware infections, data access patterns, and encrypted traffic patterns). Monitoring these scores would drive individual behavior change and provide the visibility required to address the aggregate insider threat effectively.

User Behaviors of Concern

Hiring employees costs time and money and lowers productivity while positions are unfilled and new employees learn their roles. Per-employee onboarding investments often exceed $4,000 and require up to eight months to gain full employee productivity,[34] which pressures employers to bring new employees to a productive state as soon as possible. Employers need to provide new employees with all the assets, data, and IT access necessary for them to do their job, employee productivity is a high priority. Several leading management books and best practices note that trust between management and the workforce is essential to achieve maximum productivity.[35] Whether personal or work-related, trust is critical to effective human relationships, but unearned or unwarranted trust can never be blindly assumed. Granting complete trust is more problematic in the information assurance (IA) and cybersecurity domains, where new employees very early on gain full access to critical organizational data and assets. On average, 17% of new hires depart in the first six months, and 26% leave within 12 months. Unearned trust and undue early access expose an organization to greater risk of data compromise, loss, or espionage.[36] Early trust often works out and thus promulgates the behavior. However, today the adverse impact in our highly connected world can be devastating (the average global cost per data breach is $3.6 million, the US average is over $8.6 million, with some violations exceeding $133 million. The OPM breach may approach $1 billion).[37]

Human evolution has allowed us to make sound life or death decisions in the physical world, but we are still groping for ways to recognize and counter virtual world threats.[38]

User behaviors that breach trust and compromise cybersecurity are an open research problem. A report co-sponsored by the National Institute of Standards and Technology (NIST) and the General Services Administration (GSA) found that only 26 of 789 journal articles and conference papers reviewed touched upon user behaviors. Most of these 26 lacked empirical data and specificity.[39] A review of 49 scholarly papers found similar results. Many discussed malicious insider behaviors and gave psychological explanations to help understand and detect such behavior, yet very few discussed non-malicious insider behaviors and actions that compromise security. Papers discussing non-malicious insiders focused more on user attitudes toward cybersecurity and information assurance policies without analyzing specific activities that compromise security. Understanding the psychology behind compromising user behavior is critically important, but these articles do little to help identify tangible mitigations, user accountability, or specific ways to change these troubling behaviors. A recent SANS Institute report identified causes for organizational endpoint compromise. The top reasons (representing 63% of all events) either directly or indirectly involved the internal user and the significance of the insider threat problem, and lists the following attack vectors involving the user:[40]

1. **Browser-based attacks:** visiting compromised websites that implant malware
2. **Social hacking:** clever spam messaging targeting groups or specific internal users
3. **Malicious external actors** interact with a trusting insider to gain sensitive organizational information (e.g., credentials, assets, data, or intellectual property)
4. **Ransomware:** typically delivered through organization-wide spam messages seeking at least one unwitting/malicious employee to enable the attack
5. **Credential theft or compromise:** theft or loss of an organization's asset, often stemming from carelessness in managing credentials, data, or equipment
6. **Infected, malicious USB or attached media devices** connect to the organizational IT infrastructure or connect remotely via an infected platform (e.g., home, hotel, Wi-Fi hotspot)
7. **Exploited common vulnerabilities and exposures (CVE):** disabling antivirus (AV) programs, blocking AV program updates, or preventing patch application for critical system software
8. **Compromised/unauthorized applications:** introducing compromised applications, enabling malicious software to run on corporate assets, or connecting to the organization's network via compromised off-network platforms

First published in 2008, the Verizon Research, Investigations, Solutions, Knowledge (RISK) Team Data Breach Investigations Report (DBIR) aggregated information security (IS) incident data analysis. The 2016 DBIR describes several problems directly enabled by internal user actions. Below are three of nine highlighted patterns that add context to the user risk score:

1. **Miscellaneous errors (17.7% of breaches):** 26% of these errors involved sensitive information sent to an unauthorized person, with the balance consisting mainly of internal human error or negligence.
2. **Insider and privileged account misuse (16.3% of breaches):** 34% of these were motivated by financial gain; 25% were linked to espionage.
3. **Physical theft and loss (15.1% of breaches):** 39% of these losses involved user workspace; 34% involved the user's vehicle.[41]

Based on a study of over 1,000 previous data breaches, the Software Engineering Institute (SEI) in 2016 updated best practices in reducing malicious insider risk, which is also relevant

to developing a general risk score for all internal users. We will apply most of these practices to risk areas discussed in the prior reports:[42]

Practice #1: Know and protect critical assets (and regularly evaluate who needs access)
Practice #2: Formalize an insider threat program
Practice #3: Document and consistently enforce policies and controls
Practice #4: Beginning with hiring: monitoring and responding to suspicious or disruptive behavior
    a) Perform reoccurring background investigations on staff:
        i. Criminal background
        ii. Credit Check
        iii. Social Media Sentiment Analysis
        iv. Dark Web Credential/Identity Analysis
Practice #5: Anticipate and manage negative work environment issues
Practice #6: Monitor social media activity thoroughly
Practice #7: Structure management and tasks to minimize insider stress and mistakes
Practice #8: Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees
Practice #9: Implement strict password and account management policies and practices
Practice #10: Institute stringent access controls and monitoring policies on privileged users
Practice #11: Deploy solutions to monitor employee actions and correlate information across multiple data sources
Practice #12: Monitor and control remote access from all endpoints, including mobile devices
Practice #13: Establish a baseline of normal behavior for both networks and employees
Practice #14: Enforce separation of duties and give users the least access necessary to execute their roles
Practice #15: Institutionalize system change controls
Practice #16: Close the doors to unauthorized data exfiltration
Practice #17: Develop a comprehensive employee termination program

The DoD cannot afford to wait to implement a system that enables the awareness, responsibility, and methodology to improve cybersecurity and personal accountability. The solution highlighted here lacks production-grade testing and refinement. Still, it is prompted by conclusive proof of pervasive insider threats, both malicious and other, current cybersecurity practices, well-established research, and overwhelming forensic evidence. This recommended model is the first step in a process that would evolve to meet dynamic threats as production data helps to refine the framework.

Initially, the framework will use relative scoring and subjective weighting to tie user behaviors to compromise potential. The initial stages of implementation will drive user awareness and accountability, adding empirical certainty to the risk calculation. Weights, measures, and a scoring framework will help to gather feedback and refine the process, providing management with a more reliable picture of strengths and weaknesses, and optimize framework value and predictability over time.

Between 2008 and 2018, the Verizon DBIR has consistently characterized the insider threat impact and has made it clear that organizations will continue to suffer severe consequences if this threat isn't effectively addressed. The proposed User Online Risk Score (UORS) will provide a model for measuring and managing that portion of the cybersecurity threat.

Score Components

The UORS model relies on previous research and articles organized around seven differently weighted categories and uses a maximum of 3000 points, with points subtracted from each category based upon the initial draft framework represented in Figure 1 below.

Category	Practice	Characteristics	Attributes	Score %	Points
Credential Management	Practice #10 - Implement Strict Password and Account Management Policies and Practices Practice #11 - Institute Stringent Access Controls and Monitoring Policies On Privileged Users Practice #15 - Enforce Separation of Duties and User Least Privilege Access Levels	Track Password/Credential Change History Track Password/Credential Complexity Track Password/Credential Differences Between Roles and Access Levels Track Privilege Credential Usage (Hours/Remote/Local)	I	15%	450
Asset Management	Practice #1 - Know and Protect Critical Assets (and who has access to them) Practice #13 - Monitor and Control Remote Access from All End Points, Including Mobile Devices Practice #19 - Close the Doors to Unauthorized Data Exfiltration	Track Data Copied, Moved, Uploaded, or Written to Removeable Media Track Data Copied, Moved, Uploaded, or Written During Remote Access Track Data Assets Attached Within Email Track Usage of Remote Storage (Cloud/Drop Box/Drive) Track Asset Inventory Presence and Location Track Software Update (Patch) History Track Asset Software Inventory at Appropriate Patch Level	II	20%	600
Asset Usage	Practice #2 - Develop a Formalized Insider Threat Program Practice #12 - Deploy Solutions to Monitor Employee Actions and Correlate Information Across Multiple Data Sources Practice #14 - Establish a Baseline of Normal Behavior for Both Networks and Employees	Track External Web Sites Visited Track Internal Sites Accessed Track Dark Web Access Track Login Statistics per Credential (Online/Offline/Internal/Remote) Track Assets and Data Accessed While Connected Locally Track Assets and Data Accessed While Connected Remotely Track Email Attachments Sent/Received (Uploaded/Downloaded) Track Usage Statistics of Encryption and VPNs Track AV Statistics per Credential Track Asset Intrusion/Compromise Statistics Per Credential	III	20%	600
Policy Adherence	Practice #3 - Document and Consistently Enforce Policies and Controls Practice #9 - Incorporate Malicious and Unintentional Insider Threat Awareness Into Periodic Security Training for All Employees	Track Initial Indoctrination Training Adherence Track Training Hours Track Privileged Access Agreement (PAA) Adherence Track Acceptable Usage Policy (AUP) Adherence	IV	5%	150
Work Stressors	Practice #8 - Structure Management and Tasks to Minimize Insider Stress and Mistakes Practice #17 - Institutionalize System Change Controls	Track Work Hours Track Hours Outside of Work Role Stated Norms Track Change Management Logs Track Audit and System Access Logs	V	10%	300
Work Behaviors	Practice #5 - Anticipate and Manage Negative Issues in the Work Environment Practice #20 - Develop a Comprehensive Employee Termination Program	Track Promotions, Demotions and Annual Ratings Track Work Altercations, Disagreements, and Formal Complaints Track Factors Leading to Early Transition Track Anonymously Submitted Concerns	VI	10%	300
External Behaviors	Practice #4 - Beginning With the Hiring Process, Monitor and Respond to Suspicious or Disruptive Behavior Practice #7 - Be Especially Vigilant Regarding Social Media	Periodic Background Check Periodic Credit Check Periodic Criminal Check Periodic Dark Web Identity Analysis Periodic Social Media Sentiment Analysis	VII	20%	600

Figure 1. User Online Risk Score (UORS) Model

The UORS score would measure the relative risk each user represents compared to other users within the same work role and could be used to aggregate the relative risk that a work role, group, or division represents. In this way, leadership can use this tool to allocate limited resources to prioritized areas of manageable risk. In addition, over time, an organization may choose to modify the model to address future areas of risk that become a concern after initial implementation, analysis, and mitigation efforts.

The seven categories represent areas of significant risk posed by internal users.

1. **Credential Management.** Risk related to user choices accessing corporate assets with login credentials. Scores depict usage, change statistics, and credential separation between user access roles. Low scores may indicate poor user behavior or high-risk levels associated with work roles and access to critical assets. This area could indicate suboptimal organizational processes or the need for specific training or more segregated sensitive roles and accesses.
2. **Organizational Asset Management.** This category evaluates user behaviors in accessing organizational data and maintains assigned physical assets. This category also focuses on how the user accesses, copies, and modifies data. A low score may mean the user has placed organizational data or physical assets at a higher potential for compromise, which might require modification of asset management or inventory processes.
3. **Organizational Asset Usage.** This category focuses on user behavior insofar as exposing information technology (IT) infrastructure at risk by quantifying websites visited, emails sent and received, interactions with the antivirus program, and login specifics. Low scores could indicate the possibility of an asset or data breach by an external entity who was knowingly or unknowingly assisted by the internal user. This should trigger the information security (IS) response team to take immediate actions.
4. **Information Assurance (IA) Policy.** Adherence Scores rate user risk associated with policy knowledge, training, and IA/IS auditable practices, and the need for more or specific training.
5. **Work Environment Stressors.** This focuses on user work patterns that may drive higher stress levels and increase the chance of costly accidents, apathy, or destructive attitudes. Behaviors tracked include demand signals for work outside of regular business hours, work dissatisfaction, and involvement in operational environment changes. The confluence of additional off-duty work demands and corrections to production environments can increase risk and thus require employee work-life rebalancing or changes to production modification procedures.

6. **Work Environment Behaviors.** This category measures workplace events that could increase organizational risk exposure for employees or IT infrastructure. Events such as promotions, demotions, work-related altercations, formal complaint participants, compensation actions, staff ratings, and critical life changes are tracked to determine potential risks. Low scores may indicate a need for Human Resources Department or management intervention.
7. **External User Behaviors.** This category tracks non-workplace behavior that could increase risks to the organization, staff, and customer base. A 2009 report cited some 572,000 violent crimes committed at work or on duty,[43] many detectable with a pre-employment background check or by using periodic verifications/recertifications. This category would call for routine background checks, credit reports, social media sentiment checks, and Dark Web analysis. Employee stressors change throughout life and often can have devastating impacts on the organization.

Data Capture

Data required for an initial system build is mostly aggregated metadata, which comes from the existing data source systems. The UORS model would extract processed data from other solutions and data owners. Permissions from the data owners would be required. UORS would not require the raw data, only aggregated and processed statistics, thereby reducing UORS data storage requirements to less than the original system requirements. Data for the model would be drawn from the following sources.

1. Human Resources Department managed user-specific data (i.e., background check, promotion, evaluation, salary band information, formal and anonymous complaint statistics, regular work hours)
2. Password/Credential usage statistics from the authentication and authorization (AAA) solution
3 Virtual Private Network (VPN) statistics
4. Email statistics from mail servers and local computer clients.
5. User web usage statistics
6 Network architecture statistics associated with user equipment
7 Call detail records (CDRs) from organizational cellular billing solution
8. Office phone usage and CDR statistics
9 SharePoint and other knowledge management statistics
10. Antivirus (AV) statistics
11. Intrusion detection and firewall statistics.
12. Insider threat detection statistics
13. Inventory tracking system: specific equipment assigned to and in use by the user
14. Common Access Card (CAC) management statistics.
15. Windows profile, screensaver, and host policy statistics
16. High-profile employee usage statistics
17. Training department, acceptable use policy, and IT/IA training statistics.
18 Formal trouble ticket statistics associated with the user and their equipment
19. Physical security team: badge locations, hours, and in/out statistics.
20. Audit log and change management statistics.

Score Computation

The UORS sample framework is shown in Figure 1. Examples of detailed scoring charts are shown in Figures 2, 3, and 4 within Annex A. Although each category is broken into sub-components, some highlighted items are described below:

1. To counter the previously discussed tendency to initially trust new hires, the UORS model will lower the score (indicating higher risk) for unproven new hires, who have yet to assimilate with fellow staff, policies, practices, and workplace norms.

2. Employers who allow IT access before a complete background check or without executing periodic checks (credit, police, social media sentiment, Dark Web presence) will see the risk go up for affected employees.
3. US employees tend to work longer hours than those in other developed nations.[44] Moreover, immature organizations tend to push staff to work even harder and longer. Research strongly confirms that higher hours, late-night emails, answering work calls in off-hours, and being connected to the workplace at all hours are counterproductive and costly for both the employee and employer. Working long and dynamic hours significantly increases the risk of mistakes, employee fatigue, apathy, disgruntlement, unplanned time off, higher health care costs, turnover, espionage, or vandalism. Accordingly, the UORS model would reduce scores for long hours and dynamic off-hour work duties, especially for those with elevated privileges.[45]
4. The more a privileged account is used, the higher the risk for organizations. Best practices limit such use to necessary functions, separate roles, and accounts.[46] The UORS model would include high use in the risk score. Employee overuse of a privileged account, committing espionage, or an organization plagued with bad practices would all be scored low.
5. The more a user remotely accesses the IT infrastructure, selects links within an email, or accesses external websites, the lower the UORS score will be, in order to reflect this increased risk.
6. The UORS will account for Information Technology and Information Assurance policy and practice adherence. For example, inadequate awareness or training increases user risk.

Proposed Implementation

Implementation within the DoD would occur in phases, which would combine empirical rigor with DoD-specific data. The phased approach would also add functionality and value as the model matures. The first phase would include refining and adding probabilistic rigor to the model. The second phase would address platform security, user civil liberties, and privacy concerns that may affect complete deployment. During the first two phases, limited users would interact with the model output to allow testing, refinement, and model maturation.

The third phase would expand access while incorporating feedback to increase the tool utility, user awareness, and personal accountability desired. In addition, this third phase would include the organizational risk, training teams, and management to enable more effective targeted training and corporate risk reduction. The fourth phase would be a more robust roll-out to more DoD activities and agencies. Within the last stage, a DoD enterprise-wide view would be added to enable senior DoD leader risk decisions.

CONCLUSION

The DoD invests heavily to achieve a technical overmatch with adversaries.[47] Unfortunately, in recent years this overmatch has eroded. Like the 2011 and 2015 strategies before, the 2018 Cyber Strategy lacks the specific vision and actions necessary to reverse this trend.[48] This article urges a strategy and framework implementation to more effectively address insider threats by providing an empirical measure of each user's risk through their actual behaviors. UORS will give the user near-real-time awareness of personal behaviors counter to organizational policy and cybersecurity requirements. This measure will also empower management to target training, remediation, and risk reduction while also allowing decision-makers to determine which user risk-exposed areas, roles, or practices require additional remediation more accurately. As a result, all organizational decision levels will be better able to improve cybersecurity resiliency in the face of an ever-evolving insider threat landscape, thereby collectively strengthening the DoD cybersecurity position and fulfilling the 2018 Cyber Strategy objectives.

NOTES

1. Barack Obama, "Presidential Memorandum: NITP; Minimum Standards for Insider Threat Program" (last modified 2012), https://www.dni.gov/index.php/ic-legal-reference-book/presidential-memorandum-nitp-minimum-standards-for-insider-threat-program, accessed October 30, 2018; Department of Defense, "DoD Directive 5205.16" (September 30, 2014; incorporating Change 2, August 28, 2017), http://www.dtic.mil/whs/directives (accessed October 30, 2018).
2. Department of Defense, "Assessment of the Military Services Insider Threat Programs (Redacted)" (2018), https://ogis.archives.gov/, accessed October 2, 2018, 5.
3. Department of Defense, "Summary, DOD Cyber Strategy 2018" (Washington, DC, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed October 2, 2018, 5.
4. U.S. Department of Defense, 2018, 3.
5. Charles Pfleeger, Shari Pfleeger, and Jonathan Margulies, "Security in Computing 5th Edition" (Upper Saddle River, NJ: Prentice Hall, 2015), 474.
6. Jovi Umawing, "The Enemy Is Us: A Look at Insider Threats - Security Boulevard" (last modified 2018), https://securityboulevard.com/2018/08/the-enemy-is-us-a-look-at-insider-threats/, accessed October 2, 2018.
7. Sarah Miller, "Insiders and Their Significant Others: Collusion, Motive and Concealmen" CMU SEI Insights Insider Threat Blog, last modified 2018, https://insights.sei.cmu.edu/insider-threat/2018/04/insiders-and-their-significant-others-collusion-motive-and-concealment.html, accessed October 2, 2018.
8. Department of Defense, "Assessment of the Military Services Insider Threat Programs (Redacted)," 10.
9. Obama, "Presidential Memorandum: NITP; Minimum Standards for Insider Threat Program"; John Thune, "Thune Introduces Legislation to Improve Cybersecurity Resources for Small Businesses - Press Releases - U.S. Senator John Thune" (Hon. John Thune Press Releases, last modified 2017), https://www.thune.senate.gov/public/index.cfm/2017/3/thune-introduces-legislation-to-improve-cybersecurity-resources-for-small-businesses, accessed October 2, 2018; Peter King, "Text - H.R.666 - 115th Congress (2017-2018): Department of Homeland Security Insider Threat and Mitigation Act of 2017" (Washington, DC: U.S. House of Representatives, 2017), https://www.congress.gov/bill/115th-congress/house-bill/666/text, accessed October 2, 2018.
10. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' – Foreign Policy" July 9, 2012, , https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/, accessed October 3, 2018.
11. Fran Howarth, "The Role of Human Error in Successful Security Attacks," IBM Security Intelligence, 2014, https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/, accessed October 2, 2018.
12. Ryan West et al. "Chapter IV The Weakest Link: A Psychological Perspective of Why Users Make Poor Security Decisions," In Social and Human Elements of Information Security: Emerging Trends and Countermeasures, by Manish Gupta and Raj Sharman, (Hershey, PA: Information Science Reference, 2009), http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.467.3395&rep=rep1&type=pdf, 43-60.
13. GAO, "GAO Issues Report on DOD Civilian, Contractor Workforces" (last modified 2018), https://www.gao.gov/products/GAO-18-399, accessed October 2, 2018, i.
14. Russell Rumbaugh and Heidi Peters, "Defense Primer: DOD Contractors" (2017), https://fas.org/sgp/crs/natsec/IF10600.pdf, accessed October 2, 2018, 1.
15. Department of Defense, "About Department of Defense," US Department of Defense, (last modified 2016), https://dod.defense.gov/about/, accessed October 2, 2018.
16. Varonis, "98 Must-Know Data Breach Statistics for 2021" (2021), https://www.varonis.com/blog/data-breach-statistics/ accessed June 8, 2021; Verizon, "Verizon 2021 Data Breach Investigations Report" (2021), https://verizon.com/dbir/, accessed June 8, 2021.
17. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
18. Pfleeger, "Security in Computing 5th Edition," 31.
19. Bernard Jones, "Overview DOD Defense in Depth Strategy" (no. Security 401 2005), https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident-response/106281, accessed October 2, 2018, 2-9; Dennis E. Shasha, "Defense in Depth," Scientific American (286, no. 5 (2002)), http://www.nature.com.mutex.gmu.edu/scientificamerican/journal/v286/n5/pdf/scientificamerican0502-101.pdf, accessed September 28, 2018, 101-101; Tim Bass and Roger Robichaux, "Defense-in-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations," Military Communications Conference (MILCOM 2001, Communications for Network-Centric Operations: Creating the Information Force, IEEE 1, 2001), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=985765, accessed March 23, 2014, 64-70.

NOTES

20. Jared Serbu, "Pentagon Plans New Estimates on Cost, Extent of Its Joint Information Environment," Federal News Radio (last modified 2016), https://federalnewsradio.com/defense/2016/07/pentagon-plans-new-estimates-cost-extent-joint-information-environment/ , accessed October 2, 2018; The White House, "(FY2018 Budget). INFORMATION TECHNOLOGY Table 16-1. FEDERAL IT SPENDING (2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf, accessed October 31, 2018.
21. Shane Schick, "Insider Threats Account for Nearly 75 Percent of Security Breach Incidents," Security Intelligence (last modified 2017), https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/, accessed July 25, 2018; The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy" (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, accessed October 3, 2018.
22. Jongwoo Kim, Eun Hee Park, and Richard L. Baskerville, "A Model of Emotion and Computer Abuse," Information and Management (53, no. 1 (2016)), https://ac-els-cdn-com.mutex.gmu.edu/S0378720615001019/1-s2.0-S0378720615001019-main.pdf?_tid=36a79597-4d34-45ff-8b94-aef28f9432d6&acdnat=1541043735_c5aa52fe-004188935237a18937bcd25f, accessed September 23, 2016, 91-108; Nader Sohrabi Safa and Carsten Maple, "Human Errors in the Information Security Realm – and How to Fix Them," Computer Fraud and Security (2016, no. 9 (2016)), https://www.sciencedirect.com/science/article/pii/S1361372316300732?via%3Dihub, accessed October 13, 2017, 17-20; Paul van Schaik et al., "Risk Perceptions of Cyber-Security and Precautionary Behaviour," Computers in Human Behavior (75 (2017)), https://ac-els-cdn-com.mutex.gmu.edu/S074756321730359X/1-s2.0-S074756321730359X-main.pdf?_tid=3bffb04b-1ae8-4071-b46a-322e1d7dddf4&acdnat=1541044749_2487dff92c2a072cfd34301bc4ed3734, accessed January 13, 2018, 554-559; Zinta S. Byrne et al., "From the User's Perspective: Perceptions of Risk Relative to Benefit Associated with Using the Internet," Computers in Human Behavior (59 (2016)), https://ac-els-cdn-com.mutex.gmu.edu/S0747563216300760/1-s2.0-S0747563216300760-main.pdf?_tid=7b7bdbc8-bd04-448e-a394-89fec64b7b67&acdnat=1541044970_2dc16d1826bf3e563e026b86bf4e1557, accessed August 13, 2016, 461-468.
23. Dr. Stephen A. Roberts, "Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors," Proquest Dissertations and Theses (Northcentral University, 2021), https://www.proquest.com/openview/c1c31d84698165e5843133986323a773, accessed Jan 30, 2021; Michele Maasberg and Nicole L. Beebe, "The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory," Journal of Information Privacy and Security (10, no. 2 (2014)), https://search-proquest-com.mutex.gmu.edu/docview/1691010505?OpenUrlRefId=info:xri/sid:primo&accountid=14541, accessed September 2, 2017, 59-70; Jeffrey L. Jenkins, "Alleviating Insider Threats: Mitigation Strategies and Detection Techniques," ProQuest Dissertations and Theses (The University of Arizona, 2013), https://search-proquest-com.mutex.gmu.edu/docview/1426647010/?pq-origsite=primo, accessed December 8, 2015; Asmaa Munshi, Peter Dell, and Helen Armstrong, "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents," in Proceedings of the Annual Hawaii International Conference on System Sciences, (2012), https://ieeexplore-ieee-org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6149306, accessed October 2, 2018, 2402-2411.
24. Tracey Caldwell. "Making Security Awareness Training Work." Computer Fraud & Security, (2016) https://ac-els-cdn-com.mutex.gmu.edu/S1361372315300464/1-s2.0-S1361372315300464-main.pdf?_tid=ae87b157-7199-4684-85db-b17f-710d43eb&acdnat=1541046318_a057a6f4bb396062a9dd7d4218983812, accessed October 3, 2018, 11-14.
25. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
26. Caldwell, "Making Security Awareness Training Work," 11-14; Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren, "The Positive Outcomes of Information Security Awareness Training in Companies - A Case Study," Information Security Technical Report (14, no. 4 (2009)), https://ac-els-cdn-com.mutex.gmu.edu/S1363412710000099/1-s2.0-S1363412710000099-main.pdf?_tid=75c46074-a3c0-4729-9625-86e940a5f01c&acdnat=1541046783_15b690c3eacbefc84cab970c8d5e3b4e, accessed October 2, 2018, 223-229; Steven Furnell and Ismini Vasileiou, "Security Education and Awareness: Just Let Them Burn?," Network Security (no. 12 (2017), https://ac-els-cdn-com.mutex.gmu.edu/S1353485817301228/1-s2.0-S1353485817301228-main.pdf?_tid=d7e839e-bd53-4a5b-b251-c2614ba3b1c9&acdnat=1541046892_c6c1f9cb2f9043df-9cb75a23c49d1fe1, accessed October 3, 2018, 5-9.
27. Lijiao Cheng et al., "Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory," Computers and Security, (39, no. PART B (2013)), https://ac-els-cdn-com.mutex.gmu.edu/S0167404813001387/1-s2.0-S0167404813001387-main.pdf?_tid=d2d699b5-7d55-4a16-becb-5c17e6744d02&acdnat=1541047122_926c2acae1d0290d8cb94d7f931c3c84 ,accessed October 13, 2018, 447-459.
28. Caldwell, "Making Security Awareness Training Work," 11-14.

NOTES

29. FICO, "Anatomy of a Security Rating" (2018), https://www.fico.com/en/latest-thinking/infographic/anatomy-of-a-security-rating, accessed September 13, 2018.
30. CapitalOne, "Free Credit Score; Report Check with CreditWise - Capital One," https://creditwise.capitalone.com/home , accessed October 3, 2018.
31. Tatiana Homonoff, Rourke O'Brien, and Abigail Sussman, "Does Knowing Your FICO Score Change Financial Behavior? Evidence from a Field Experiment with Student Loan Borrowers (SSRN, 2018), https://wagner.nyu.edu/files/faculty/publications/Homonoff%2C O%27Brien%2C and Sussman 2-23-17.pdf , accessed October 3, 2018, 22-24.
32. CapitalOne, "Free Credit Score; Report Check with CreditWise - Capital One".
33. Homonoff, "Does Knowing Your FICO Score Change Financial Behavior?" 22-24.
34. Society for Human Resource Management, "2017 Talent Acquisition Benchmarking Report" (2017), https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2017-Talent-Acquisition-Benchmarking.pdf, accessed January 27, 2019, 4, 9, 13, 15; Aleks Peterson. "Hidden Costs of Onboarding a New Employee" (2018), https://www.glassdoor.com/employers/blog/hidden-costs-employee-onboarding-reduce/, accessed January 28, 2019.
35. Dori Meinert, "Why Trust Matters at Work"(2018), https://www.shrm.org/hr-today/news/hr-magazine/0618/pages/why-trust-matters-at-work.aspx, accessed January 27, 2019); Paul Towers, "Workplace Trust: Why Trust Is Important In The Workplace," (2017), https://blog.taskpigeon.co/workplace-trust-trust-important-workplace/, accessed January 27, 2019.
36. Society for Human Resource Management, "2017 Talent Acquisition Benchmarking Report"; Clover, "Enterprise behavior: Reduce the cost of employee onboarding" (2018), http://blog.clover.com/better-business/enterprise-behavior-reduce-the-cost-of-employee-on-boarding/, accessed January 28, 2019; Aleks Peterson. "Hidden Costs of Onboarding a New Employee"; Andrew Mcllvaine, "Does new-hire onboarding take too long—or not long enough?" (2018), http://hrexecutive.com/curing-onboardings-ailments/, accessed January 28, 2019.
37. Dell Technologies & Intel, "Data breaches cost US businesses $7M - Business Insider" (2017), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4, accessed March 6, 2018; IBM & Ponemon Institute, "Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study" (2017), https://www.prnewswire.com/news-releases/ibm--ponemon-institute-cost-of-a-data-breach-dropped-10-percent-globally-in-2017-study-300476378.html, accessed January 28, 2019; Broadcom, "OPM Breach Costs Could Exceed $1 Billion"(2017), https://community.broadcom.com/groups/communities/community-home/librarydocuments/viewdocument?DocumentKey=ea860f79-10aa-4707-870c-6f0ef1cdd3da&CommunityKey=638e24fb-cc43-455a-9185-c8a0130c2076&tab=librarydocuments, accessed June 10, 2021.
38. N. Davinson & E. Sillence, "It won't happen to me: Promoting secure behaviour among internet users", Computers in Human Behavior, (26(6), 2010). https://doi.org/10.1016/j.chb.2010.06.023 , accessed January 27, 2019, 1739-1747; V. Dutt, Y.S. Ahn, & C. Gonzalez, "Cyber Situation Awareness," Human Factors: The Journal of the Human Factors and Ergonomics Society, (55(3), 2013), https://doi.org/10.1177/0018720812464045 , accessed January 27, 2019, 605-618; L. Tomczyk & K. Kopecký, "Children and youth safety on the Internet: Experiences from Czech Republic and Poland," Telematics and Informatics, (33(3), 2016), https://doi.org/10.1016/j.tele.2015.12.003, accessed January 27, 2019, 822-833.
39. S. Boyson, T. Corsi, & H. Mann, The Cyber Risk Predictive Analytics Project: A NIST and GSA Sponsored Project Principal Investigators (2017), https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/UMD Final Report-Cyber Risk Analytics Project revised tc november 25 2017.pdf, accessed January 28, 2019.
40. L. Neely, "Endpoint Protection and Response: A SANS Survey;" SANS Institute Survey (2018), www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827, accessed January 28, 2019.
41. Verizon, "2016 Data Breach Investigations Report", Verizon Business Journal, (1, 2016), https://doi.org/10.1017/CBO9781107415324.004, accessed January 28, 2019, 1-65.
42. M.L. Collins et al., Common Sense Guide to Mitigating Insider Threats. 5th Edition (December 2016), https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf, accessed January 28, 2019, xii, 6, 11-123.
43. H.L. Chou & C. Chou, "An analysis of multiple factors relating to teachers' problematic information security behavior," Computers in Human Behavior, (65, 2016), https://doi.org/10.1016/j.chb.2016.08.034, accessed January 28, 2019, 334-345.
44. G.E. Miller, "The U.S. is the Most Overworked Nation in the World," (2018), https://20somethingfinance.com/american-hours-worked-productivity-vacation/ , accessed January 28, 2019; Sarah Carmichael, "The Research Is Clear: Long Hours Backfire for People and for Companies" (2015), https://hbr.org/2015/08/the-research-is-clear-long-hours-backfire-for-people-and-for-companies, accessed January 28, 2019.

NOTES

45. Ibid: Leslie Perlow & Jessica Porter, "Making Time Off Predictable and Required," HarvardBusinessReview (2019), http://web.b.ebscohost.com.mutex.gmu.edu/bsi/pdfviewer/pdfviewer?vid=1&sid=f4101167-14b8-4ce4-97a3-504d004fe56e%40sessionmgr120 , accessed January 28, 2019.
46. M.L. Collins et al. (2016), Common Sense Guide to Mitigating Insider Threats, 5th Edition (December 2016), xii, 6, 11-123.
47. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
48. Ibid.; Department of Defense, "DoD Cyber Security Strategy" (2015), http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (accessed October 2, 2018); Department of Defense, "Strategy for Operating in Cyberspace" (2011), http://books.google.com/books?hl=en&lr=&id=YTOY-2jPXoiQC&oi=fnd&pg=PA1&dq=Department+of+Defense+Strategy+for+Operating+in+Cyberspace&ots=KJvSm-cJY-b&sig=LBdHoKpQlvqRzkb8zIGrVmRScEo, accessed October 8, 2014.

ANNEX A – *UORS Detail Scoring Charts*

I

Value	MAX (460) MIN(-800)	Target
	Credential Change History	100
100	Average of >= 6 times in previous 12 months	
60	Average of >= 3 times in previous 12 months	
0	New User or less than 12 months of history	
-100	Average of >= 1 times in previous 12 months	
-200	Less than 1 time in previous 24 months	
	Credential Reuse History	60
60	Last >= 18 credentials unique (previous 36 months)	
20	>= 9 credentials unique (previous 36 months)	
0	New User or less than 36 months of history	
-100	>=3 credentials unique (previous 36 months)	
-200	no unique credentials (previous 36 months	
	General Credential Complexity	100
100	Complexity within information security (ISIA) policies	
-100	Complexity NOT within information security (ISIA) Policies	
	General Credential Creation Methodology	200
200	Two-factor general credential usage within A policy	
60	Password generation and storage solution (non two factor)	
-100	User generated passwords only	
	Privilege Credential Creation Methodology Usage Deductions	0
0	Not applicable	
-26	Two-factor general credential usage within A policy	
-100	Password generation and storage solution (non two factor)	
-200	User generated passwords only	
	Privilege Credential Complexity Deductions	0
0	Not applicable	
-26	Complexity within information security (ISIA) policies	
-200	Complexity Not within information security (ISIA) policies	
	Credential Separation of Roles Deductions	0
0	Not Applicable - only one role	
-100	Separation of normal and privileged credentials	
-500	Co-mingled credential usage used for privileged and general roles	
	Privileged Credential Usage Deductions	0
0	Not applicable	
-40	Average < 10 hours per month (current rolling 12 months)	
-80	Average of < 25 hours per month (current rolling 12 months)	
-100	Average of < 50 hours per month (current rolling 12 months)	
-200	Average of >= 50 hours per month (current rolling 12 months)	
	Remote General Credential Usage Deductions	0
0	Not applicable	
-26	Average of < 2 hours per month (current rolling 12 months)	
-40	Average of < 6 hours per month (current rolling 12 months)	
-60	Average of < 15 hours per month (current rolling 12 months)	
-100	Average of >= 15 hours per month (current rolling 12 months)	
	Remote Privileged Credential Usage Deductions	0
0	Not applicable	
-60	Average of < 2 hours per month (current rolling 12 months)	
-80	Average of < 6 hours per month (current rolling 12 months)	
-100	Average of < 15 hours per month (current rolling 12 months)	
-200	Average of >= 15 hours per month (current rolling 12 months)	
	High Profile Role (VP and Up/Public Profile) Deductions	0
0	Not applicable	
-26	All communications managed by segregated "office of" accounts	
-60	Unmanaged separation of internal and external credentials	
-200	Co-mingled credential usage used for internal and external applications	

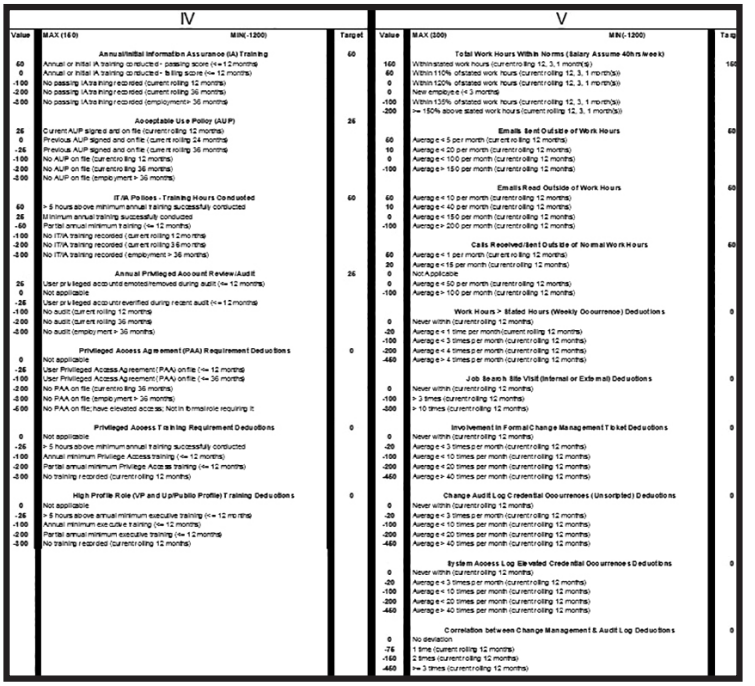
II

Value	MAX (800) MIN(-800)	Target
	Asset Software Inventory Per Credential	80
80	Asset SW (including removed) matches inventory requirements	
60	Expected deviation requiring inventory update	
-10	Minor unapproved deviation	
-100	Major deviation (asset with potential critical data missing)	
	Asset Software Patching Audit Per Credential	80
80	All asset SW inventory at approved patch/release level	
0	Expected small deviation requiring update	
-100	Major deviation (>1 patch level, >1 release level or >1 SW package)	
	Asset Inventory and Location Statistics Per Credential	26
26	All asset inventory tied to credential at location/IP within last week	
0	Asset inventory not at location/IP for more than 3 weeks	
-100	Asset inventory not at location/IP for more than 10 weeks	
	Data Writes to Mass Storage (USB/CD/DVD/Remote storage)	76
76	No data writes to removable/remote mass storage	
0	Authorized writes removable/remote mass storage	
-100	Unauthorized writes removable/remote mass storage	
	Data Reads from Mass Storage (USB/CD/DVD/Remote storage)	76
76	No data reads from removable/remote mass storage	
0	Authorized reads from removable/remote mass storage	
-100	Unauthorized reads from removable/remote mass storage	
	Data Reads from Internal Storage (Shares/SharePoint/Lan)	60
60	Data reads from internal storage within 110% of work role norm	
0	Data reads from internal storage within 125% of work role norm	
-100	Data reads from internal storage above 140% of work role norm	
	Emails Sent with Attachments (To External Entities)	60
60	Email attachment data size within 110% of work role norm	
0	Email attachment data size within 125% of work role norm	
-100	Email attachment data size within 140% of work role norm	
	Emails Received with Attachments (From External)	40
40	Email attachment data size within 110% of work role norm	
0	Email attachment data size within 125% of work role norm	
-100	Email attachment data size within 140% of work role norm	
	Organizational Data and Assets Accessed Remotely	60
60	Data/Assets within 110% of work role norm (hours/location/type)	
0	Data/Assets within 125% of work role norm (hours/location/type)	
-100	Data/Assets within 140% of work role norm (hours/location/type)	
	Attempts to Access Data or Assets Not Authorized Deductions	0
0	All data assets authorized	
-50	10% of data/assets accessed unauthorized (hours/location/type)	
-100	20% of data/assets accessed unauthorized (hours/location/type)	
-200	>= 30% of data/assets accessed unauthorized (hours/location/type)	

III

Value	MAX (800) MIN(-1200)	Targ
	External Web Sites Visited	40
40	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Number of Non-Governmental Websites Visited	60
60	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Number of Governmental Web sites Visited	10
10	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Amount of Time Spent Visiting External Web sites	80
80	# Minutes expected within 110% of work role norm (hours/location/type)	
0	# Minutes expected within 125% of work role norm (hours/location/type)	
-100	# Minutes expected >= 140% of work role norm (hours/location/type)	
	Internal Web Sites Visited	10
10	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Emails Sent During Work Hours	100
100	# Email sent within work role norms (hours/location/type)	
70	# Email sent within 110% of work role norm (hours/location/type)	
20	# Email sent within 125% of work role norm (hours/location/type)	
0	# Email sent within 136% of work role norm (hours/location/type)	
-100	# Email sent >= 150% of work role norm (hours/location/type)	
	Asset Antivirus Statistics Per Credential	76
76	Clean AV scan (with latest AV update) (current rolling 12 months)	
60	< 6 files detected (current rolling 12 months)	
36	< 8 files detected (current rolling 12 months)	
0	< 12 files detected (current rolling 12 months)	
-200	> 12 files detected (current rolling 12 months)	
	Asset Compromise Intrusion Detection Per Credential	126
126	No detected compromise (current rolling 12 months)	
-100	1 detected compromise (current rolling 12 months)	
-200	> 1 detected compromise (current rolling 12 months)	
	Local Credential Statistics (Logged into Organizational Assets)	26
26	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Remote Credential Statistics (Logged into Organizational Assets)	26
26	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Usage of VPN connected to corporate assets from external	60
60	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Dark Web Access Attempt Deductions	0
0	No detected attempts (current rolling 12 months)	
-200	1 Visit detected (current rolling 12 months)	
-500	> 1 Visit detected (current rolling 12 months)	
	Web browsing Tied To Privileged Credential Deductions	0
0	No detected usage (current rolling 12 months)	
-200	1 Browsing event detected (current rolling 12 months)	
-500	> 1 Browsing event detected (current rolling 12 months)	
	Web Links Selected From Email Deductions	0
0	No detected usage (current rolling 12 months)	
-100	1 Attempt detected (current rolling 12 months)	
-200	> 1 Attempt detected (current rolling 12 months)	
	Email Sent or Read Using Privileged Credentials Deductions	0
0	No detected usage (current rolling 12 months)	
-200	1 Attempt detected (current rolling 12 months)	
-500	> 1 Attempt detected (current rolling 12 months)	
	Usage of VPN/Encryption Connected To External Sites Deductions	0
0	# Minutes accessed within 110% of work role norm (hours/location/type)	
-40	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Screensaver Idle Time Setting Deductions	0
0	# Minutes <= A policy/GPO setting	
-26	# Minutes above A policy/GPO setting by < 5 minutes	
-100	# Minutes above A policy/GPO setting by >= 5 minutes	
	CAC Left in Computer After Screensaver Deductions	0
0	# Minutes after screensaver < 30 min avg/week (rolling 3 months)	
-40	# Minutes after screensaver < 60 min avg/week (rolling 3 months)	
-100	# Minutes after screensaver < 90 min avg/week (rolling 3 months)	
-200	# Minutes after screensaver >= 120 min avg/week (rolling 3 months	

Figure 2. UORS Categories I, II, & III Scoring



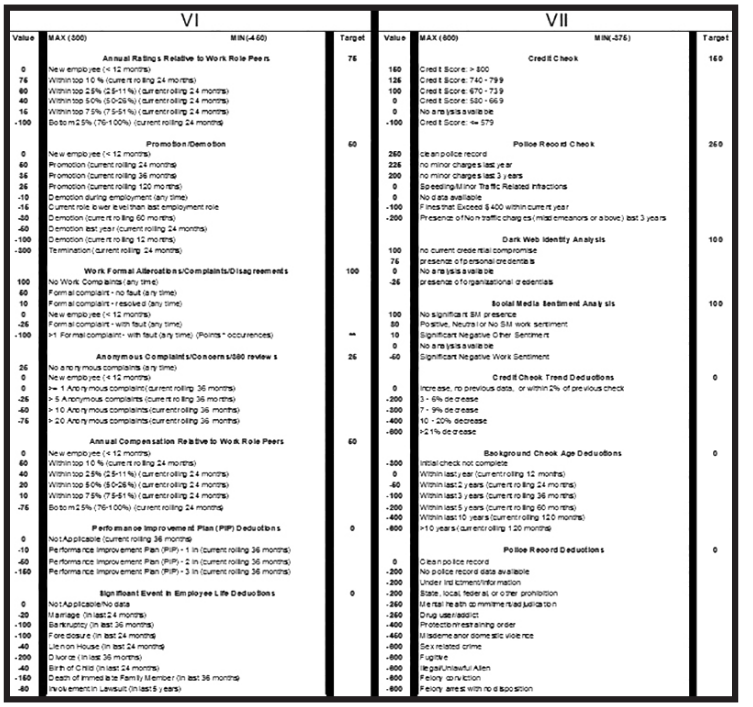
IV

Value	MAX (160) MIN(-1200)	Target
	Annual/Initial Information Assurance (IA) Training	60
60	Annual or Initial IA training conducted - passing score (<= 12 months)	
0	Annual or Initial IA training conducted - failing score (<= 12 months)	
-100	No passing IA training recorded (current rolling 12 months)	
-200	No passing IA training recorded (current rolling 36 months)	
-500	No passing IA training recorded (employment> 36 months)	
	Acceptable Use Policy (AUP)	26
26	Current AUP signed and on file (current rolling 12 months)	
0	Previous AUP signed and on file (current rolling 24 months	
-26	Previous AUP signed and on file (current rolling 36 months)	
-100	No AUP on file (current rolling 12 months)	
-200	No AUP on file (current rolling 36 months)	
-500	No AUP on file (employment > 36 months)	
	ITA/ Policies - Training Hours Conducted	60
60	> 5 hours above minimum annual training successfully conducted	
26	Minimum annual training successfully conducted	
-60	Partial annual minimum training (<= 12 months)	
-100	No ITA training recorded (current rolling 12 months)	
-200	No ITA training recorded (current rolling 36 months)	
-500	No ITA training recorded (employment > 36 months)	
	Annual Privileged Account Review/Audit	26
26	User privileged accounts/ entitlements reviewed during audit (<= 12 months)	
0	Not applicable	
-26	User privileged accounts/ entitlements reviewed during recent audit (<= 12 months)	
-100	No audit (current rolling 12 months)	
-200	No audit (current rolling 36 months)	
-500	No audit (employment > 36 months)	
	Privileged Access Agreement (PAA) Requirement Deductions	0
0	Not applicable	
-25	User Privileged Access Agreement (PAA) on file (<= 12 months)	
-100	User Privileged Access Agreement (PAA) on file (<= 36 months)	
-200	No PAA on file (current rolling 36 months)	
-500	No PAA on file (employment > 36 months)	
-600	No PAA on file; have elevated access. Not in timeframe requiring it	
	Privileged Access Training Requirement Deductions	0
0	Not applicable	
-26	> 5 hours above minimum annual training successfully conducted	
-100	Annual minimum Privilege Access training (<= 12 months)	
-200	Partial annual minimum Privilege Access training (<= 12 months)	
-500	No training recorded (current rolling 12 months)	
	High Profile Role (VP and Up/Public Profile) Training Deductions	0
0	Not applicable	
-26	> 5 hours above annual minimum executive training (<= 12 months)	
-100	Annual minimum executive training (<= 12 months)	
-200	Partial annual minimum executive training (<= 12 months)	
-300	No training recorded (current rolling 12 months)	

V

Value	MAX (300) MIN(-1200)	Targ
	Total Work Hours Within Norms (Salary Assume 40hrs/week)	
160	Within stated work hours (current rolling 12, 3, 1 month(s))	160
60	Within 110% of stated work hours (current rolling 12, 3, 1 month(s))	
0	Within 120% of stated work hours (current rolling 12, 3, 1 month(s))	
0	New employee (< 3 months)	
-100	Within 130% of stated work hours (current rolling 12, 3, 1 month(s))	
-200	>= 150% above stated work hours (current rolling 12, 3, 1 month(s))	
	Emails Sent Outside of Work Hours	60
60	Average < 5 per month (current rolling 12 months)	
10	Average < 20 per month (current rolling 12 months)	
0	Average < 100 per month (current rolling 12 months)	
-100	Average > 150 per month (current rolling 12 months)	
	Emails Read Outside of Work Hours	60
60	Average < 10 per month (current rolling 12 months)	
10	Average < 40 per month (current rolling 12 months)	
0	Average < 150 per month (current rolling 12 months)	
-100	Average < 200 per month (current rolling 12 months)	
	Calls Received/Sent Outside of Normal Work Hours	60
60	Average < 1 per month (current rolling 12 months)	
20	Average < 15 per month (current rolling 12 months)	
0	Not Applicable	
0	Average < 50 per month (current rolling 12 months)	
-100	Average > 100 per month (current rolling 12 months)	
	Work Hours > Stated Hours (Weekly Occurrence) Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 1 time per month (current rolling 12 months)	
-100	Average < 3 times per month (current rolling 12 months)	
-200	Average < 4 times per month (current rolling 12 months)	
-460	Average > 4 times per month (current rolling 12 months)	
	Job Search Site Visit (Internal or External) Deductions	0
0	Never within (current rolling 12 months)	
-100	> 3 times (current rolling 12 months)	
-500	> 10 times (current rolling 12 months)	
	Involvement in Formal Change Management Ticket Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-460	Average > 40 times per month (current rolling 12 months)	
	Change Audit Log Credential Occurrences (Unscripted) Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-460	Average > 40 times per month (current rolling 12 months)	
	System Access Log Elevated Credential Occurrences Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-460	Average > 40 times per month (current rolling 12 months)	
	Correlation between Change Management & Audit Log Deductions	0
0	No deviation	
-76	1 time (current rolling 12 months)	
-160	2 times (current rolling 12 months)	
-460	>= 3 times (current rolling 12 months)	

Figure 3. UORS Categories IV & V Scoring



VI

Value	MAX (500) MIN(-460)	Target
	Annual Ratings Relative to Work Role Peers	76
0	New employee (< 12 months)	
76	Within top 10 % (current rolling 24 months)	
60	Within top 25% (25-11 %) (current rolling 24 months)	
40	Within top 50% (50-26 %) (current rolling 24 months)	
16	Within top 75% (75-51 %) (current rolling 24 months)	
-100	Bottom 25% (76-100%) (current rolling 24 months)	
	Promotion /Demotion	60
0	New employee (< 12 months)	
60	Promotion (current rolling 24 months)	
36	Promotion (current rolling 36 months)	
26	Promotion (current rolling 120 months)	
-10	Demotion during employment (any time)	
-16	Current role lower level than last employment role	
-30	Demotion (current rolling 60 months)	
-60	Demotion last year (current rolling 24 months)	
-100	Demotion (current rolling 12 months)	
-300	Termination (current rolling 24 months)	
	Work Formal Altercations/Complaints/Disagreements	100
100	No Work Complaints (any time)	
60	Formal complaint - no fault (any time)	
10	Formal complaint - resolved (any time)	
0	New employee (< 12 months)	
-26	Formal complaint - with fault (any time)	
-100	>1 Formal complaint - with fault (any time) (Points * occurrences)	**
	Anonymous Complaints/Concerns/360 reviews	26
26	No anonymous complaints (any time)	
0	New employee (< 12 months)	
0	>= 1 Anonymous complaint (current rolling 36 months)	
-26	> 5 Anonymous complaints (current rolling 36 months)	
-40	> 10 Anonymous complaints (current rolling 24 months)	
-75	> 20 Anonymous complaints (current rolling 36 months)	
	Annual Compensation Relative to Work Role Peers	60
0	New employee (< 12 months)	
60	Within top 10 % (current rolling 24 months)	
40	Within top 25% (25-11 %) (current rolling 24 months)	
20	Within top 50% (50-26 %) (current rolling 24 months)	
10	Within top 75% (75-51 %) (current rolling 24 months)	
-75	Bottom 25% (76-100%) (current rolling 24 months)	
	Performance Improvement Plan (PIP) Deductions	0
0	Not Applicable (current rolling 36 months)	
-10	Performance Improvement Plan (PIP) - 1 in (current rolling 36 months)	
-60	Performance Improvement Plan (PIP) - 2 in (current rolling 36 months)	
-160	Performance Improvement Plan (PIP) - 3 in (current rolling 36 months)	
	Significant Event in Employee Life Deductions	0
0	Not Applicable/No data	
-20	Marriage (in last 24 months)	
-100	Bankruptcy (in last 36 months)	
-100	Foreclosure (in last 24 months)	
-40	Lien on House (in last 24 months)	
-200	Divorce (in last 36 months)	
-40	Birth of Child (in last 24 months)	
-160	Death of Immediate Family Member (in last 36 months)	
-80	Involvement in Lawsuit (in last 5 years)	

VII

Value	MAX (600) MIN(-376)	Target
	Credit Check	160
160	Credit Score: > 800	
126	Credit Score: 740 - 799	
100	Credit Score: 670 - 739	
0	Credit Score: 580 - 669	
0	No analysis available	
-100	Credit Score: <= 579	
	Police Record Check	260
260	clean police record	
226	no minor charges last year	
200	no minor charges last 3 years	
0	Speeding/Minor Traffic Related Infractions	
0	No data available	
-100	Fines that Exceed $400 within current year	
-200	Presence of Non-traffic charges (misdemeanors or above) last 3 years	
	Dark Web Identity Analysis	100
100	no current credential compromise	
76	presence of personal credentials	
0	No analysis available	
-26	presence of organizational credentials	
	Social Media Sentiment Analysis	100
100	No significant SM presence	
80	Positive, Neutral or No SM work sentiment	
10	Significant Negative Other Sentiment	
0	No analysis available	
-60	Significant Negative Work Sentiment	
	Credit Check Trend Deductions	0
0	Increase, no previous data, or within 2% of previous check	
-200	3 - 6% decrease	
-300	7 - 9% decrease	
-400	10 - 20% decrease	
-600	>21% decrease	
	Background Check Age Deductions	0
-300	Initial check not complete	
0	Within last year (current rolling 12 months)	
-60	Within last 2 years (current rolling 24 months)	
-100	Within last 3 years (current rolling 36 months)	
-200	Within last 5 years (current rolling 60 months)	
-400	Within last 10 years (current rolling 120 months)	
-600	>10 years (current rolling 120 months)	
	Police Record Deductions	0
0	Clean police record	
-200	No police record data available	
-200	Under Indictment/Information	
-300	State, local, federal, or other prohibition	
-260	Mental health commitment/adjudication	
-260	Drug user/addict	
-400	Protection/restraining order	
-460	Misdemeanor domestic violence	
-600	Sex related crime	
-600	Fugitive	
-600	Illegal/Unlawful Alien	
-600	Felony conviction	
-600	Felony arrest with no disposition	

Figure 4. UORS Categories VI & VII Scoring

Lessons for the DoD when Planning for the Future of S&T

Lieutenant Colonel (P) Natalie Vanatta, Ph.D.
Alex Ruiz

ABSTRACT

Telling the future is not yet possible, but we have nearly come to expect it, thanks to incredible achievements in technology which presents us with an ever-improving sense of what is probable. This has introduced interesting challenges, for example, when DoD prepares for future states of the world. This was a challenge recently undertaken by researchers at OUSD (R&E), where a glimpse into science and technology out to the year 2045 was explored as part of a Congressionally mandated report included in the 2020 NDAA. A credible team of experts was commissioned for the effort, who additionally organized a complement of technology analysts and writers. A parallel project was conceptualized and nominated by a few researchers who felt it important to investigate the thoughts and perspectives of professionals whose worldview is dominated by such matters: futurists, technology forecasters, and science fiction writers. Thus, the OUSD (R&E) Principal Director for Cyber agreed to launch Project Valence (the namesake being a nod to the gregarious nature of valence electrons); the members of which successfully reached a dozen such luminaries, and recorded nearly 30 hours of unbridled exploration about the world to come. Notably, regardless of whether visions prove to be true, such a world will undoubtedly feature a fighting force charged with the defense of America, comprised of experts many of whom have not yet been born.

Lieutenant Colonel (P) Natalie Vanatta is a U.S. Army Cyber officer and an Academy Professor at the Army Cyber Institute, United States Military Academy. Here she focuses on bringing private industry, academia, and government agencies together to explore and solve the cyber challenges facing the U.S. Army over next 3-10 years. She holds a Ph.D. in applied mathematics as well as degrees in computer engineering and systems engineering. Natalie has also served as a Distinguished Visiting Professor at the National Security Agency, technical director to Joint Task Force Ares, and team leader within the Cyber National Mission Force.

25 YEARS OUT IS FAR

> "...And so, I should say that 2045, for me, is a little far, to be honest. And so I'm going to go outside of my comfort zone, because I do 10 years out. So, this means that you must do the forecasting and envisioning of the future differently with different voices. Because the range is so far, that **you really are going to trip into the impossible, you're going to trip into the fact that well, that couldn't happen. [But] when you get right up to the edge of the impossible, you've got the possible, right?**"
>
> *- Brian David Johnson*[1]

It is an enormous task to think so far out in the future and expect to get anything right. Up until the 20th century, the future unfolded in fairly predictable ways for most people, who tended to live similar lives across a couple of generations, and where "quantum leaps" in lifestyle-changing technology or other disruptions might be experienced every 100 years.

Generations would pass, and the circumstances that affected people would remain somewhat static. Certain discoveries caused disruptions, such as the aqueduct and the printing press, and numerous weapons and tactics that, when adopted, would change the expected outcomes of wars in some cases. But the lives people generally led and the opportunities they experienced tended to only change in slight, incremental ways that were as detectable to them as the movement of glaciers. The future was not as tangible to people then, and futurists of the time provided more entertainment than anything else.

This idea of slow and metered change seems to adequately describe life in the past and yet, it is undeniably an inaccurate description of modern life. The information age is characterized by major shifts in lifestyle changes occurring numerous times inside a single

Alex Ruiz is an advisor to the DoD on Information and Cyber Warfare, a Nonresident Senior Fellow at the Atlantic Council, and founder of Phaedrus LLC, a private engineering company specializing in professional, tailored systems engineering practices to bridge gaps between government acquisitions and agile processes known to the private sector. Alex has written and co-written publications on information environment strategy, combating disinformation, how cyber enables influence operations, and how science and technology will shape our future. Also, a Cyberspace Warfare Officer in the Air Force Reserve, Lt. Col. Alex Ruiz employs his operational experience across mission needs of the US Air Force's Information Warfare Command (16th Air Force) and at U.S. Cyber Command. In all matters, Alex seeks solutions for geopolitical competition and conflict, studying the nature and character of war as humankind finds its way into a future shaped by increasingly uncertain circumstances. Alex holds an MS degree in Systems Engineering from Johns Hopkins University and a BA in History from Norwich University.

generation and with disruptions that can upend markets and entire nations without warning. The combination of smartphones and socially-oriented applications, for example, have brought us increasingly extreme examples of semi-orderly but rather effective "flash campaigns," which range in effect from the mass uprising of the Arab Spring in 2011 to the decentralized amalgamation of disorderly interests that came together in the January 6th riot and insurrection at the U.S. Capitol in 2021. On a more metaphysical, but all the while equally concerning front, the deliberate manipulation of stock prices in the case of the GameStop "meme" stock frenzy of 2021 shows that deliberately disruptive activity need not include active physical violence, but could still pose insidious threats to order across the global financial system. These and many other worldwide events demonstrate that technology and the flow of information have outpaced collective government understanding, leaving political leaders and strategists confused on how to keep pace with these unceasing changes. Nefarious actors abound, looking to exploit what have become key digital frontlines shaping the nature and character of global competition and conflict.

In the information age, a person can experience a drastically changing world, the changes of which unfold without warning numerous times across one's lifetime leaving many to feel like they are hanging on to the rear bumper of a world as it fishtails through these hyperactive rates of change; bringing uncertainty, anxiety, and tension along in the wake. The Department of Defense (DoD) has learned to take notice, but there is a new problem. Whereas the static nature of futurism in generations past involved a high degree of fantastical speculation, the circumstances of today have established conditions where there is a dire need to make such speculations. The permutations of potential futures can cause a sense of analytical paralysis, partly because there are too many plausible futures to consider, resulting in an increased opportunity to present

inaccurate views. For example, speculative conversations on the future of quantum computing can evoke an array of non-committal opinions from experts in terms of the likelihood of its implications on national security (particularly in terms of timelines and level of detriment). This has resulted in an inconsistent narrative and a broader lack of appreciation for what achievements in this area of research will mean to people. Attempting to tell this future is risky for experts because the actual state of the situation will be observable in their lifetime and their assertions could be visibly proven wrong.

Some of this is considered more a reflection of our inability to think exponentially, coupled with the phenomenal game-changer that is the modern information environment, with its unending, radically increasing offerings of knowledge. This, in turn, has become somewhat of a grand equalizer for the masses in terms of the proliferation of ideas and concepts which might otherwise be kept as state secrets. An empire might hold significant advantages over this new world for generations if able to control information within its borders. Keeping secrets is exceedingly difficult, and the ubiquitous presence of sophisticated computers allows the average person to make great use of what was otherwise only interesting information. The culmination is rapid change across the world and a clearer sense on how the future will unfold in ways we can observe and experience outside of novels, comic books, and movies.

Therefore, the military and the government must evolve how it thinks about the future and the range of possible and potential threats in multiple futures—an undertaking requiring considerable time, effort, and inclusion from modern theorists such as technology forecasters, futurists, and science fiction writers. To get at what is possible, we first need to think about what seems impossible and walk backwards a little. This thinking will provide a broader range of potentials to contemplate as traditional military planning and strategic planning are necessary but insufficient for the 21st Century. If we do not change the way we think about the future, how we talk about it, and who is forecasting (i.e., with respect to age, gender, ethnicity, domain specialty), we will suffer from a failure of imagination and the resulting inability to comprehend what we can affect in the present. This failure of imagination is a failure of national security and carries potentially catastrophic consequences.

TEAM VALENCE

Amid the pandemic challenges and the political turbulence brought about in the last Presidential election, the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E) carried out a little-known effort to predict the future of science and technology. Tasked by Congress, the organization had to produce a Science and Technology (S&T) roadmap spanning the coming quarter of a century (note: a separate article featuring the resulting S&T roadmap, still under edit at this time, is anticipated closer to its release in late spring 2022).

Supported by a team of writers, analysts, engineers, and other technical minds, OUSD (R&E)'s Principal Director for Cyber (serving as the effort's primary office of responsibility and

roadmap's signatory) also looked for support beyond the Pentagon to help explore less common perspectives not bound by programmatic and budgetary cycles (PPBE, FYDP, etc.). After a couple of academic discussions regarding the more philosophical points on thinking and writing about the future, a small team devised a plan to use their collective networks to help gather such perspectives from expert futurists, forecasters, and science fiction writers. Project Valence—a self-defined group of "free radicals, orbiting the outer shell of the DoD," looking to make strong bonds with external audiences in pursuit of the broadest view possible on matters of the future—was born out of this. Valence, a collective of hackers with technical backgrounds who had found their way into industry, the Defense Digital Service, as faculty at West Point, and a Senior Fellow at the Atlantic Council, were excited to provide the Pentagon new insights into what the future of technology could look like and how it could affect future military operations. Valence was in a direct position to assist OUSD (R&E) with what would become, for itself, a rather unconventional approach of reaching out to veritable strangers, holding semi-structured interviews, and exploring the minds of modern-day oracles to reset how one part of the Pentagon thinks about the future.

> "It occurred to us that there is a natural inclination for roadmap projects and for the professionals that conduct them to focus on technology in timeframes that relate too closely with programmatic budgetary epochs like the FYDP (Future Years Defense Program) and the POM (Program Objective Memorandum) Cycle. We live in that space, and so departing it is an active and deliberate exercise which would prove critical to exploring the world out to 2045."
>
> *– Alex Ruiz, Project Valence researcher*

Based on the team's collective decades of experience within DoD, they were aware of many doctrinal writings, strategies, flight plans, roadmaps, etc., that had failed to accomplish their intended purpose. Many of these thoughtful and thoroughly prepared works ultimately offered platitudes about the most critical national security challenges and offered minor changes (e.g., a new cup holder for a fighter jet) to current technical capabilities as the solution. Their common flaw was that they neglected to obtain a deeper sense of the layered problems of global conflict and the broader matters which cause wars to happen, along with their limited understanding of the insane speed of technological development and adoption in this Century.

To bring a different view of the future to the Pentagon, Valence first organized these layers into three distinct axes. These axes provide a framework to understand what the next 25 years may look like, showing what science and technology capabilities might be necessary to accomplish the DoD's mission. Using outside voices helped the team re-think the typical military approach to the future and technology.

Axis I dealt with natural and phenomenological matters—the independent variables to which humankind is wholly reactive. The obvious ones are climate change and pandemics, but other events such as extra orbital incursions from asteroids, volcanoes, or other potential cataclysmic

events were considered. These variables were examined in the context of the existential challenges and the corresponding forcing function such events play in demanding human cooperation on a grand scale.

Axis II centered on the psychosocial responses of humankind as they pertain to our orientation and behavior triggered by events from Axis I. Billions of people's collective reaction to the stressors of living in an unpredictable environment make up most of the story about the life of humans on Earth. Telling stories is central to the human experience. We craft narratives based on the human condition, positioning ourselves at their center, often with the hopeful outlook of heroic triumph over impossible odds. In the context of global challenges, the notion of Axis II was that humankind could either exacerbate resulting challenges from Axis I through matters of competition and conflict or rise heroically above them through cooperation and coalition. And indeed, there would be much to either fight over or collectively work to overcome. Climate change, for example, will undoubtedly create conditions of failed crops, uninhabitable spaces, and displaced persons (especially in considering the combination of Axis I phenomena and Axis II failures)—which we are already struggling to bear witness to at the southern US border, for example. Valence considered an extrapolation of these and other conditions as they play out around the world, intensifying in volume and urgency from now to 2045, stressing governments and constituents, and calling for solutions to the growing number of people stranded without a country and in search of survival. All of these things, and a range of other such matters left to chance, will cause suffering, induce competition and conflict, and lead to circumstances compelling the US to intervene, setting future challenges for an increasingly stressed DoD.

"The best way to predict the future is to invent it!"

–Alan Kay[2]

And of course, Axis III, which is meant to be injected into the aforementioned lines of thinking and driving a central question: Can the choices we make with science and technology (S&T) help us produce desirable outcomes amid the aforementioned challenges?

"The best way to predict the future...is to prevent it."

–Alan Kay

More specifically, can DoD use S&T to reduce the suffering introduced by both nature and humankind's orientation to its challenges? And, in so doing, could we bend the arc of US (and therefore, global) futures such that we all but eliminate most reasons for committing kinetic warfare, reducing, or perhaps eliminating our need to send younger generations into physical combat? In previous generations, such thinking might have been met with ire, but the US (and the civilian and military leadership of DoD) is poised for a moment of clarity after two decades of fighting in the Middle East. Combined with the notion of Axis I dangers already setting conditions for Axis II incursions (refugee crises, pandemic-triggered scarcity, contested water

sources), Valence encapsulated the notion of reducing suffering while realizing that S&T could exacerbate conflict as much as alleviate it, and that the choices we make now have critical implications on where we end up in 2045.

Beyond the questions regarding the plight of weapon systems and nature and character of war, Valence wanted to understand if the DoD could:

1) Introduce the idea of thinking "to, and through" conflict

2) Understand the potential origins of future fighting

3) Solve it like treating technical problems in advance of complex systems failures

This bit of guided thinking brought the team to a period of planning and internal literature review. Matched with the validating wisdom of renowned experts, Valence sought to make sense of a world whose future had been wrapped in a growing abundance of information but a lack of meaning for many.

The team embraced Dr. Alan Kay's notions about inventing the futures we desired and preventing the ones we do not. However, these notions would remain an enduring challenge of the project—namely, gaining the diversity of thought (from outside the DoD or defense industrial base) to think about the technological challenges and solutions in the next quarter of a century. Like many government agencies, DoD is strongly influenced by retired military officers reprising their professional worldview as civil servants; and the defense industrial base is motivated by selling things to the DoD. While neither of these influences is inherently wrong, they do tend to stifle innovation and thinking, particularly because the two worlds combine with a third in the planning, programming, budget, and execution (PPBE) cycle creating a small universe that consumes most thinking to compete for limited fiscal resources. Ideas of the future, particularly the lofty, must survive immediate resource fights of the "here and now."

To help confront what prospective readers might assume is a Pentagon-produced report on what the future of S&T through 2045 might look like, Valence reached out to experts for a counter-voice. The team created a notional list of futurist luminaries each member could potentially get some time with. List in hand, the team then developed a basic structure for collaborative discussions that would go for hours, all conducted in late evenings so that the team could free its collective mindset for some rather unique and unconventional conversations. Valence members took turns leading the dialogue, and all members took turns presenting questions. All respondents agreed to have the sessions recorded, and an application was used to sort through each one, creating transcripts of the events. Within a few days of each occurrence, the team would collaborate on analysis papers to help distill important points and draw conclusions to aid with the ongoing OUSD (R&E) roadmap (known as the 2021 NDAA, Section 257 report) development. Right away, the team achieved its objective—a giant leap out of the terrestrial confines of DoD future speculation, into the deep and odd questions regarding the state and nature of the world and what life will be like for us in years to come.

The following sections of this article are highlights from the aforementioned Project Valence interviews, each offering some critical concepts that we must pay attention to over the next quarter of a century. They mostly revolve around misconceptions and underlying assumptions that permeate typical military futures thinking. The experts that Valence interviewed brought these ideas to life. Ultimately, the DoD (and even the wider US Government) should incorporate these ideas into their future wargames, simulations, and development of strategies and roadmaps to ensure that our military continues to develop and invest in the S&T capabilities that will meet our needs in the future.

THE FUTURE IS LOCAL

> "And it turns out, actually, that the future is different depending upon where you live, because the future is local. There is no one global future to plan for."
>
> *–Brian David Johnson*

The future happens where you are. Often when people think about the future, it is flawed thinking because they can only imagine that it happens "over there," as if the future happens in Washington DC or Moscow or Beijing or Norway but not in their home. But the fact is that the future happens where you are: all futures are local.

Indeed, spending a day in Seoul and the next in Dhaka can show you how the future unfolds differently for different people and that where you are matters. For example, the future of privacy looks very different in the continental US versus the European Union versus Russia versus China. These fundamental differences directly relate to worldviews, competition, and play a major part in the potential for conflict.

In creating the S&T roadmap, the OUSD (R&E) team was challenged to plan and prepare for the future, yet their standard assumption was that the future would be "a" future that linearly progresses. While scenarios used in the roadmap addressed different threat types to tease out specific technological aspects of the future operating environment, they still followed the same future progression. This is typical of military thinking, where one path to the future is selected, and then the effort is focused on developing plans and capabilities to succeed on this path, minimizing alternatives. Additionally, this limits practical reasoning and expectation not to consider how other nations/societies will embrace visions of the future, instead to assume that the US-centric mentality will hold across the globe.

Adopting the mindset that the future is not a global future, but a local future will help drive a sense of the underlying issues we must be more prepared to engage with. In the combined stressors of budgetary austerity, hyperpolar information and cyber conflict, aggressor nations and regional hegemony, and the imminent threat of climate change, the DoD will be unable to respond symmetrically to every failed matter of geopolitics. The picking and choosing that planners and decision-makers will have to do will be eternally dependent on understanding

the Axis II matters of people and culture and any underlying Axis I phenomenology potentially bringing out the worst in humankind.

As DoD thinks about how the S&T investments in cyber over the next decade unfold, one element that can help disambiguate the synchronous multi-verse problem is the reminder that S&T presents incredible opportunities to help level playing fields between population centers experiencing the least desirable of these futures. For generations, the US has observed struggles in far-flung parts of the world and responded with limited charity and humanitarian aid. The current state of technology offers unprecedented opportunities to help underserved communities gain sustainable footholds across the basic matters of survival: electricity, water, food, and shelter. A major change agent that will help illuminate paths to success for all populations is information technology, which is undergoing its latest chapter of expansion in the form of higher throughput for urban areas and increasing overall reach to far-flung areas thanks to expanded broadband programs and the prospect of space-based internet provisioning projects like Starlink. Vast communications infrastructures that bring the ultimate public library to the hands of anyone with a capable device can and will ultimately bring about progress if we take Joy's law of management[3] to heart.

We must consider that the future not only plays out differently depending on where one lives on Earth, but that technology going forward allows for some degrees of freedom in designing the reality to unfold. Considering this unevenness, and that lack of opportunity contributes to conflict, it is important to understand the state of the world in aggregate beyond our borders.

THE CHARTER TO GET THINGS RIGHT HAS BEEN WRITTEN: THE PLIGHT OF FAILED AND FAILING STATES IN THE FUTURE

> "Roughly **a third of the world's countries** are what would be called **failing states** by any set of measures, for example from the Fragile States Index or the World Population Review, with almost **another quarter on the verge of failure.** And these are the countries where a lot of wars of contagion will occur. Many of them will be internal wars, though sometimes they'll bleed over to involve other nations, as the Congo war that killed 5 million did. These conflicts should matter to us, in terms of trying to prevent or deter them, or at least to respond effectively to them. Because they have led, and will continue to lead, disproportionately, to terrible, terrible human suffering."
>
> *–Dr. John Arquilla*[4]

As DoD looks at the investments they should make over the next few decades in the cyber S&T spaces, it is essential to also think about where DoD assets might be deployed in that same time period. As stated by then-Secretary of Defense Robert Gates to a class of West Point cadets in 2011, "when it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right, from the Mayaguez to Grenada, Panama, Somalia, the Balkans, Haiti, Kuwait, Iraq, and more– we

had no idea a year before any of these missions that we would be so engaged."[5] This trend becomes increasingly concerning as the future of failing states should give us pause. We should not be planning for a Fulda Gap remix or the "classic blunder of land war in Asia."[6] Still, we could be called on as a peace-keeping force or humanitarian aid providers around the globe in small countries where our adversaries are attempting to co-opt and take advantage of their dire circumstances. These are the same small countries that will benefit or suffer from the evolution of and deployment of technology. How, with a small force, can we deter our adversaries in competition before conflict in a location that, potentially, we never saw coming?

The US will continue to face the same adversaries over the next two decades (the 2+3),[7] but must embrace and harness S&T to achieve its political and military aims in ways unlike the previous two decades. As such, the DoD should expect to employ forces in new locations/countries, accept and embrace new ways to present task-organized and/or force structure, which accounts for the sharply increased cyber capabilities we will need in the future. This holds especially true in terms of electromagnetic spectrum implications inherent in our pivot away from the austere "last mile" challenges of Southwest Asia to the dense backdrop of digital noise present across rising areas of interest in the Indo-Pacific. Complex operations we have mastered in one part of the world do not readily translate to others (e.g., LTE, 4G, trusted 5G, non-trusted 5G, authorized spectrum bands, or trusted/non-trusted telecommunications infrastructure). Considering that global trends show a sustained increase in cyber and information warfare, these classes of assets should, from now on, be regarded as foundational to fighting conflict as runways, fighters, bombers, and carrier battlegroups have been. Investment in these technologies and an extreme focus on integrating cyber and electronic warfare capabilities are required to ensure that we can compete in the active warfighting domain of our time, and help to define norms that reduce the circumstances of a hostile information environment.

FUTURE CONFLICT SOURCES

> "If anything, the next 10 years will be really sorting out how do we operate in this world. And if we wanted to hedge our bets and get ahead on future conflicts, I would be **investing in as much technology as possible to make abundant things that are currently not abundant, such as water, food, and electricity. If you can make those things abundant**, then you remove sources of future conflict."
>
> *–Dr. David Bray*[8]

> "**And the simple fact is, every new abundance creates an adjacent scarcity**. So if you want to look for the scarcities you're gonna fight over, look at what's next to the new abundance."
>
> *–Paul Saffo*[9]

DoD's mission, as the largest USG agency, is to provide the military forces needed to deter war and ensure our nation's security.[10] The DoD has continued to adapt to an overall declining

state of physical conflict since World War II, but an increasingly multi-polar, and now hyper-polar threat environment in terms of armed nation-states, low-intensity conflict, and what will undoubtedly be a continued rise in trans-national threats such as narco-terrorists, complex criminal syndicates, hacking groups, and cyber weapons proliferation and trading across the dark web. These threats represent a significant increase in potential destabilization, and all such elements are being further stressed by climate change. DoD will have to consider these concepts alongside their more traditional undertakings, such as: confronting nuclear-armed states and their outlying threat rings of kinetic weapon systems. Ultimately, interventions across all conceivable domains of conflict will be required to secure a future state recognizable to us (today) in terms of Western, democratic values.

The DoD needs to consider how it will combine focusing on developing and purchasing the next generation of tanks, fighter jets and aircraft carriers while also developing technology and promoting scientific research which can adequately affect the survival needs of the lowest level of others around the globe. Simply put, a world where a third of nations are failed states, with another major tranche on the brink, is a net failure for everyone, most certainly in the recognition that climate change will create challenges that defy political borders. Alleviating these matters results in a direct payoff here at home, but this notion can be hard to sell.

The US is engaged in a great power competition. It has become increasingly clear that our adversaries wish to shape a world consistent with their authoritarian model by gaining authority over other nations' economic, diplomatic, and security decisions. This occurs most readily when small nations are struggling with scarcities that our adversaries offer in abundance. As part of the DoD's mission to ensure our nation's security, we must realize some S&T investments create capabilities that achieve military objectives on the battlefield could have a dual-use purpose of balancing the playing field in other countries during competition.

WHAT DO WE WANT FROM TECH?

> "What we're building right now is a whole bunch of Russian sailors. We're training our AI systems to do exactly what they are told when they are told to do it and not to think. What we really **want to do is build a whole bunch of 1943 farm boys from Iowa,** who see something and can improvise the living daylight out of it because of what they understood."
>
> *–John-Francis Mergen*
>
> "When will we have a robot give a bath to an elderly person at home?"
>
> *–John Markoff*[11]
>
> "...whenever we have a new technology, we always use the new technology to pave the cowpaths...to do some new thing in an old way. And, that gets me to what we're doing today is the ultimate cow-path-paving technology. We're using the power of the web and the awesome processing power on our desktops to simulate in a really inefficient way...

to march backwards into the future. You know, **let's let technology be truly novel.**"

–Paul Saffo

One of the most considerable challenges regarding S&T investment is to first pause and analyze what we really want from S&T. Twenty years from now, what do we want technology to be able to do for us? And, perhaps more broadly, what do we want the world to be like?

As children, the Jetsons[12] gave us a possible view of the future world full of advanced, digital technology. It was a world of push-button simplicity. Everything could be done with the push of a button in 2062 (the notional calendar year for the Jetsons). That is all that George does all day (all 3 hours) at work, and all that Jane needs to do to keep the household running. And yet, we were also introduced to Rosey, the robot maid – the imperfect, humanoid robot helper that did all the things that needed more than a push of the button. Just as Hanna-Barbera studios had to make conscious design choices on what activities would be acceptable for a robot or technology to perform and what activities still needed a human to action, DoD must spend resources (time and thinking) to explore what are acceptable activities for future technology and where we are still uncomfortable ceding control to a machine or piece of code.

Then, as was mentioned previously in this article, imagination must be let loose. We must journey to the edge of the impossible and let loose the shackles of societal convention to think about what we want technology to actually do for us. Consider this the "inverse" problem. Technology does not have to be constrained to only automating today's processes or performing incremental improvement on today's capabilities; instead, it has the potential to be game-changing—if only we can imagine it. However, before we can truly develop a comprehensive game plan for future S&T investments, we need to understand what we want that S&T to be able to produce.

AI IS A JOURNEY OF DECADES WITH AN UNTOLD FUTURE

"So, the history of the steam engine is actually the history of a technology that evolved over a 100-year cycle from its first rudimentary stationary form built to evacuate water out of mines...to becoming a mobile train, to developing into a railway system, to re-defining our concept of time, to influencing how utilities were distributed across the nation. Today's AI is like yester-year's steam engine. When it becomes a system (and not a piece of technology), that will be exciting. Because all the technology that you're imagining is still stuck on it being inside a computer and so people are failing to grasp it because they are so mesmerized by the impossibility. But the **world that is coming is infinitely more complicated** because what will happen when AI is no longer bound inside the object or talking to each other?"

–Dr. Genevieve Bell[13]

Whether you consume your news from the television or the internet, there is a seemingly endless discussion about Artificial Intelligence (AI) and how it will save the day. Vendors are

hawking it in their products to increase your productivity, and for-profit universities are offering degrees in it so that you can weather this new coming age of intelligence as your old job will be replaced by machines and software. When faced with a future changing at an ever-increasing rate, it is easy to get caught up in the rip current and just accept that AI will be ready to save us and make it all better (or that the great AI borg will consume us all, and that resistance is futile). At present, AI applications often echo history when snake oil was sold as a cure-all elixir for many kinds of physiological problems in the 18th and 19th Centuries. Unfortunately, we now know that this panacea failed to solve the health problems that it was marketed against and, in fact, just worsened many of these health problems as individuals failed to use other means to combat their ills. So, can we really expect AI to solve all our problems in the future?

The answer is maybe, but probably not at the timeline that current vendors proclaim. AI is not new: it was a concept first coined in 1955 by John McCarthy roughly as, the goal of AI is to develop machines that behave as though they were intelligent.[14] It is now 60+ years after the original work, and we are still unsure of when AI will really arrive. A much more elegant definition of AI is from Elaine Rich: "AI is the study of how to make computers do things at which, at the moment, people are better."[15] This manifested in 1955 when Arthur Samuel (IBM) developed a learning algorithm that could play checkers better than its developer to 2016 when AlphaGo beat one of the world's best Go players. AI science takes time and remains an elusive reality compared to Dick Tracy's watch and flying cars (for some reason, Maxwell Smart's shoe phone never seemed to penetrate the market). Therefore, to imagine that AI will be here tomorrow to solve our world challenges is a bit too optimistic. However, we also can't just ignore it until it gets here because of the profound impacts on society and life. To quote the Space Balls,[16] "when will then be now?" Perhaps when a robot can improvise Gershwin tunes on a violin alongside human jazz players, that might be a vital clue. When said robot creates novel things never done on a violin in the same situation, one can probably be certain.

Though the steam engine took decades to manifest, it still had profound impacts around the globe: from developing the concept of standard time (and time zones), determining how major transportation and communication infrastructure would be employed within the US (thereby creating have and have not zones). None of these global effects were imagined by the creators of the steam engine. Similarly, it is hard to picture the potential effects that AI will have on humankind. This yields the difficult problem of preparing to use a technology (and respond to an adversary's use of this technology) without knowing what this technology can do and when it will be available. Therefore, we must continue to invest in both the science and the technology that support the development of AI systems (as outlined in the upcoming OUSD (R&E) roadmap) and acknowledge that DoD must diversify its portfolio of technological solutions to best support the military. Even when the general AI arrives, it will probably create new problems/challenges that we cannot begin to fathom today.

HUMAN-MACHINE TEAMING

> "...humans have been having conflicts for multiple millennia. Looking ahead, what do we still not know about human nature that could trip us up in the next future? My guess right now is, **we still don't fully understand how human nature will respond to ubiquitous advanced technologies**, which are fundamentally alien to how evolution has shaped our behaviors as a species."
>
> *–Dr. David Bray*

It seems that an unstated assumption within DoD is a take on "if we build it, they will come"[17] —namely, that if we build the S&T capability, then it will be helpful and used by humans. Imagine an early caveman being introduced to the wheel (an alien thing and beyond their normal comprehension of the world's capabilities). How many iterations of this technology were necessary until he became comfortable with it? How many iterations of use were necessary until he found the best way to use it? So, it seems that many are assuming that if new cyber capabilities are built, they will be instantly valued, useful, and comfortable within a military context.

Yet, there is still a great need for thinking and researching the best way for humans to team up with machines to build a productive partnership. These concepts must be included in developing future cyber capabilities that operators will need and want to use. Indeed, one can think of it as creating a symbiotic relationship with technology—to enable it to be more like an R2-D2 to our Luke (favored over the clunky Boolean-dependent C3PO from Star Wars).

Research shows that humans need three things to trust an entity (whether that is trusting another human being or a machine): that the entity is benevolent, competent, and operates with integrity.[18][19] If those features can be included in the design, then a pathway is created for a human to trust the capability. Because if you think that they are benevolent, you will probably form a friendship with them. If you think they are competent, you will treat them as an expert system. If you believe they have integrity, you are not worried about what they will do with your data or information. To effectively team, the entities must trust each other.

Additionally, until now (in human history), there have been very few technologies that extend humans' cognitive capabilities and their ability to operate at a scale beyond their physical reach. Humans are good at building tools that are mechanical and adapting to them. But aside from books and possibly some psychedelic drugs, altering one's mental state is new to us. A typical conversation with the various SMEs that Valence talked to would include a warning to proceed a little bit cautiously with human-machine teaming. Namely because a lot of what we see right now with domestic polarization in the US, Europe, and elsewhere clearly demonstrates inept understanding of the impact of today's tools on our cognitive abilities, let alone be able to comprehend the potential impact of tomorrow's capabilities.

So, building trust in cyber capabilities and envisioning how teaming will occur with operators must be a vital component of the scientific research and application development from the initial

design phase of the capabilities. Developing this understanding of how humans will respond to technology might be the difference between success and failure in the future, given that, now more than ever, we will look to technology for answers about our most vexing problems.

CLIMATE AS A RAVISHING AFFECT

> "DoD is not a capitalist enterprise; It is effectively a non-profit—it uses the money given to get the job done that it has been assigned to do without worrying about whether it will make a profit in the end. So, it is an exemplary organization: highly competent, good esprit de corps, really good wage parity, and working on protecting the country... **DoD is the largest non-profit in the world.**"
>
> *–Kim Stanley Robinson*[20]

In a thought-provoking conversation with Kim Stanley Robinson right after the release of his new book "The Ministry for the Future", he challenged our understanding of what the DoD actually is. To not just think of the organization as employing almost 3 million service members and civilians to defend the nation, but to think of the organization as the largest non-profit in the world. Considering that the DoD is not constrained by a need to make money and its "shareholders" are the American people, we can lead the world in a hopeful new direction. Making the world a safer place makes America a safer place.

As the previous generation of DoD leaders faced the quasi-existential threat of the Russians pouring through the Fulda Gap, today and tomorrow's leaders face an actual existential threat of climate change. It will radically change how the DoD envisions military operations and prepare for them across the DOTMLPF-P[21] spectrum. Climate change threatens to compromise cities/regions/countries and inflict severe and irreversible harm to almost every aspect of society, creating failed states and increased sources of conflict across the globe. A whole-of-world approach is needed but at least the US can start with a whole-of-government approach and be the moral leader in this space. The DoD is uniquely positioned to do so within the US government due to its resources, authorities, influence, partnerships, and sheer size. The real challenges are those of foresight and wisdom, which are required to mobilize the will of the American people to understand that situations of suffering beyond our borders are incubators of tomorrow's wars, some of which will involve our armed forces. There could be no better spokesperson than the DoD regarding the net cost of such failed circumstances and how to avoid them.

Some elements within the DoD S&T/R&D community are already working towards solutions that directly address the most pressing drivers of climate change. The DoD uses a tremendous amount of energy. While this number has been dropping since 1975,[22] the Department still uses more energy than any other single entity on the planet. To combat this reliance on fossil fuels and reduce the military's carbon footprint, the Services initiated several projects to increase efficiency. For example, the Navy's Geothermal Program Office (EXWC PW68) is a

leader in geothermal resource care and exploration within the DoD. They explore, develop, and maintain geothermal energy production sites for the Navy and the DoD. Similarly, the other service components have long-standing research programs that could positively affect climate change if their successes were embraced and incorporated on a national scale. In recognition of the impact of climate change on national security[23] and the need for results, the DoD Climate Action Team stood up earlier this year to translate thoughts into action.[24]

As the threat looms nearer and more significantly, the window of opportunity for humanity to respond is quickly disappearing, and the necessity of intervention from the DoD becomes greater. The DoD cannot remain solely focused on purchasing the next generation of aircraft if, within a decade, we might not have the fuel to fly them anymore.

MILITARY CULTURE IS AN UNSOLVED PROBLEM

> "Therefore, perhaps the question is not what is the future but what are our sacred cows? Those things that we won't get rid of. Those organizational and/or political roadblocks that are going to keep us from adopting well or innovating or changing. And that requires soul searching for people."
>
> *–P.W. Singer*[25]

Both the US and its nation-state adversaries have the problem of relying on decades of military culture to make decisions about the future. However, the US should rely more on what basic science tells us, and the answer will probably be in the middle. Therefore, as we craft the roadmap to the future, it will be a significant problem to also get the narrative correct so that we can start to overcome the inertia of military culture that might hinder the development of capabilities that will save future lives on the battlefield or spare us from battle altogether.

It is not just about choosing the right cyber capabilities to invest in over the next two decades, but also about how we choose to use them once they arrive. The worry is that we will be like the British in the 1920s. Then, it was not about whether you used the tank and the airplane in battle, but about how you used them. The British invented the tank and the aircraft carrier. They conducted phenomenal wargames to test the technology's best employment within operations but did not choose the best employment concept because of their own military culture. Military history is rife with examples of failing to implement new technology correctly because the current culture could not imagine doing things differently and actively worked against embracing new ideas. Therefore, even if the DoD develops a perfect roadmap to investing in S&T capabilities over the next couple of decades, if they fail to overcome the long-standing inertia of military culture, that failure might hinder the use of capabilities that will save future lives on the battlefield. This holds especially true in that broader DoD does has not recognized that Cyber and IW will represent how most fighting will unfold in the future, and that there is a more logical conclusion to be drawn that JDAMs will probably not be needed as we shift our gaze to Indo-PACOM.

The influence of US military culture is also seen in the argument of quantity versus quality—especially as it plays into technology. A significant risk to the DoD is that the combination of military culture and the defense economy has been quality-focus dominant for the past 75 years. The irony is that this is the opposite of what we did in World War II to win; the US made durable, high-utility systems (akin to Jeeps) but now make exquisite, fragile systems similar to Ferraris. But as we look at autonomous robotics (in the air, sea, and land) and swarming tactics, Ferraris do not seem to be the way to go. The fear is that even if the most innovative military planners and technologists determine that swarms would be better to accomplish anticipated military objectives, it is unclear whether the Pentagon could ever convince itself to purchase enough to make it profitable for the defense contractors to offer. The contractors will most likely peddle the Pentagon on the amazingness of six big, expensive platforms. Then the generals will be surrounded by contractors explaining how effective the big ones are, and there will be no marketplace offering the small ones which meet our tactical needs. Therefore, reworking the military and defense sector culture might be a key component to realizing and embracing our future S&T needs.

Ultimately, the sacred cows are the military's unconscious bias(es), which are based on decades of experience in a risk-averse model. If the DoD refuses to picture a future where they will have to change, they will be caught by surprise and at a devastating disadvantage if the adversaries can let go of their sacred cows.

WHAT IF WE DO NOT INVEST IN SCIENCE AND TECHNOLOGY?

A recent example of the cost of second-rate technology on the battlefield is the 43-day Nagorno-Karabakh war. This was a short and largely unacknowledged part of a decades-old Caucasus conflict that unfolded in late 2020 in a region fought over by Armenia and Azerbaijan (the territory is internationally recognized as part of Azerbaijan). Armenia suffered a crushing defeat against the Turkish-backed Azerbaijanis, who made massive investments in Turkish and Israeli unmanned aerial vehicle technology in the years leading up to the war. Armenia showed up to fight with old tactics and Cold War-era field weapons (tanks and artillery pieces).

Blending well-crafted deception tactics and integrated systems, Azerbaijanis used decoys (old An-2 biplanes retrofitted with remote piloting capability, thought to have been acquired from Ukraine) to lure out Armenia's mobile air defenses in a kind of pilotless Wild Weasel suppression of enemy air defense (SEAD) campaign. The actual UAV fleet, Turkish Bayraktar TB2, and Anka-S combat drones loitered at higher vantage points and observed the defense positions, swarming the Armenians and issuing a sweeping, punishing defeat over nearly 180 separate battles. According to a Turkish analyst from the Istanbul-based Center for Economics and Foreign Policy Studies (EDAM), what was showcased by Azerbaijan on the battlefields of the Karabakh region extended from Turkish-provided doctrine published on robotic warfare and concepts of operations.

The Azerbaijanis adopted other tactics from Turkish, Russian, and US playbooks, including the use of small agile field forces akin to Special Operations contingents and small bands of advanced operational nodes dubbed "saboteur groups," somewhat like the curious case of "little green men" present during Russia's 2014 aggression in Crimea. The combination of battlefield losses, air superiority provided by highly integrated and capable UAVs, fissures created by the saboteur groups that helped ensure target fixes, and the use of laser targeting technology made for a case of overwhelming force that resulted in Azerbaijan's successful takeover of large parts of the Karabakh region before a cease-fire was declared.

The Nagorno-Karabakh story is one of successful systems and tactics integration, and of timely and effective investments in S&T. Moreover, what is known about Azerbaijan's investment in these technologies includes the rapid acquisition of these and other systems in 2018, meaning that the intense and very rapid planning and engineering over two years put them in place to utterly dominate a comparatively stone-age rival. Extrapolating on this a little further, what this conflict should teach us is that the kill chain is much broader than typically referred. Comprising S&T, R&D, build and development, implementation, and fielding, and beyond, these are matters which must be honed and compressed to gain and maintain the cascading advantages advanced technology can provide.

CONCLUSION

Now more than ever, we must expect the unexpected. And so, writing about the future has become a crucial exercise that allows us to consider what we will need to confront in terms of threats, not only as it pertains to the future of the United States, but to a world favoring Western, Democratic values. Whereas conflicts of the recent past have been the ones easiest to assess, the DoD will be pushed to acknowledge that planning for and fighting according to lessons learned of previous wars is a losing business model, and there will be less tolerance for lack of foresight as our interconnected, technological world offers us the ability to do predictive analysis. Easy as that is to accept, what must come next is a changed way of thinking across the DoD that is insistent on sensing the causes of conflict and understanding how adversaries will engage, across physical and metaphysical domains alike, and amid the stressors and pressures of ultimate pacing threats such as climate change and the cascading challenges which will result. The pace of such matters is staggering, and the rates of change in norms and aspects of conflict will continue to vex planners and decision-makers. But, if we tune into the thoughts and curiosities of those who live in this particular head-space – the futurists, technology forecasters, and science fiction writers – we can ground ourselves in important elements critical to understanding these abstract challenges. Namely, that the future is local, that we can and should seek to invent the future as we desire, and that deliberate prevention of a world we wish for others not to inherit should be thought of as within our span of control. We need only commit ourselves to the required levels of cooperation, understanding, of course, that our species has not yet proven its ability to do that quite yet.

NOTES

1. Brian David Johnson, Arizona State University, accessed July 11, 2021, https://csi.asu.edu/people/brian-david-johnson/.
2. Alan Kay, Wikipedia, accessed July 20, 2021, https://en.wikipedia.org/wiki/Alan_Kay.
3. Manville, Book. "How To Get The Smartest People In The World To Work For You" *Forbes*, accessed September 10, 2021, https://www.forbes.com/sites/brookmanville/2015/07/24/how-to-get-the-smartest-people-in-the-world-to-work-for-you/?sh=4a1c99fa2f21.
4. John Arquilla, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/John_Arquilla
5. https://www.americanrhetoric.com/speeches/robertgateswestpointspeech.htm.
6. Rob Reiner, dir., *Princess Bride*, 1987 (Beverly Hills, CA: MGM, 2013), DVD.
7. See: Summary of the 2018 National Defense Strategy of the United States of America, accessed July 20, 2021, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf or https://www.defense.gov/Explore/Spotlight/National-Defense-Strategy/.
8. David Bray, Atlantic Council, accessed July 11, 2021,https://www.atlanticcouncil.org/expert/david-bray-phd/.
9. Paul Saffo, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/Paul_Saffo.
10. About, DoD, accessed July 11, 2021, https://www.defense.gov/our-story/.
11. ohn Markoff, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/John_Markoff.
12. *The Jetsons,* Season 1 Directed by William Hanna & Joseph Barber, aired September 23, 1962, to March 17, 1963 on ABC.
13. Genevieve Bell, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/Genevieve_Bell.
14. Wolfgang Ertel, *Introduction to Artificial Intelligence* 2nd edition, Springer, 2017.
15. Elaine Rich, "Artificial Intelligence and the Humanities." *Computers and the Humanities* 19, no. 2 (1985): 117-22, accessed August 3, 2021. http://www.jstor.org/stable/30204398.
16. Mel Brooks, dir., Spaceballs, 1987 (Beverly Hills, CA: MGM, 2012), DVD.
17. Phil Alden Robinson, dir., *Field of Dreams*, 1989 (CA: Universal Studios, 2003), DVD.
18. Jack Zenger and Joseph Folkman, "The 3 Elements of Trust" *Harvard Business Review* (2019), accessed August 3, 2021. https://hbr.org/2019/02/the-3-elements-of-trust.
19. "The Three Elements of Trust,"Transcend Management Advisors Inc, accessed August 3, 2021, https://transcendmgt.com/the-three-elements-of-trust/.
20. Kim Stanley Robinson, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/Kim_Stanley_Robinson.
21. "DOTmLPF-P Analysis", Defense Acquisition University, accessed July 11, 2021, https://www.dau.edu/acquipedia/pages/ArticleContent.aspx?itemid=457
22. "Defense Department energy use falls to lowest level since at least 1975," U.S. Energy Information Administration (February 2015), accessed July 11, 2021, https://www.eia.gov/todayinenergy/detail.php?id=19871.
23. "Energy Action Month Puts Spotlight on DoD Efforts," U.S. Department of Defense, accessed on July 11, 2021, https://www.defense.gov/Explore/News/Article/Article/1972916/energy-action-month-puts-spotlight-on-dod-efforts/.
24. "Action Team Leads DoD Efforts to Adapt to Climate Change Effects," U.S. Department of Defense, accessed on July 11, 2021, https://www.defense.gov/Explore/News/Article/Article/2577354/action-team-leads-dod-efforts-to-adapt-to-climate-change-effects/.
25. P.W. Singer, Wikipedia, accessed July 11, 2021, https://en.wikipedia.org/wiki/P._W._Singer.

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

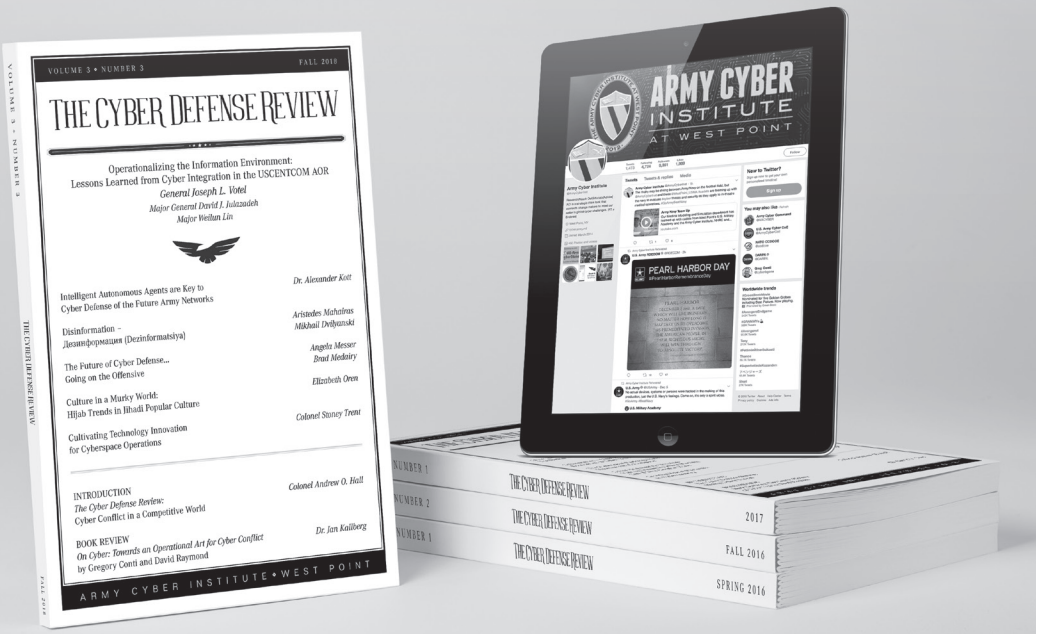
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



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.