

# THE CYBER DEFENSE REVIEW

## An Offensive Future?

Guest Editors

*Dr. Andrew C. Dwyer and Dr. Amy Ertan*



### Prepare and Prevent, Don't Repair and Repent: The Role of Reinsurance in Offensive Cyber

*Alicia Bates*

### Exploit Brokers and Offensive Cyber Operations

*Matthias Dellago, Andrew C. Simpson, Daniel W. Woods*

### Democracies and the Future of Offensive (Cyber-Enabled) Information Operations

*Dr. Bryan Nakayama*

### Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations

*Ewan Lawson*

### Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations

*Dr. Nori Katagiri*

### The Failure of Offense/Defense Balance in Cyber Security

*Dr. Brandon Valeriano*

### The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity

*Dr. Joe Burton*

### Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking

*Dr. Rod Thornton, Dr. Marina Miron*

---

#### INTRODUCTION

An Offensive Future?

*Dr. Andrew C. Dwyer*

*Dr. Amy Ertan*



# THE CYBER DEFENSE REVIEW

◆ SPECIAL EDITION ◆



# THE CYBER DEFENSE REVIEW

## A DYNAMIC MULTIDISCIPLINARY DIALOGUE

### EDITOR IN CHIEF

Dr. Corvin J. Connolly

### MANAGING EDITOR

Dr. Jan Kallberg

### ASSISTANT EDITORS

West Point Class of '70

### ARMY CYBER INSTITUTE

Col. Jeffrey M. Erickson  
Director

Dr. Paul Maxwell  
Deputy Director

Sgt. Maj. Amanda Draeger  
Sergeant Major

Dr. Edward Sobieski  
Senior Faculty Member

Col. Stephen S. Hamilton, Ph.D.  
Chief of Staff

### AREA EDITORS

Dr. Harold J. Arata III  
(Cybersecurity Strategy)

Dr. Michael Klipstein  
(Cyber Policy/Cyber Operations)

Dr. David Raymond  
(Network Security)

Lt. Col. Todd W. Arnold, Ph.D.  
(Internet Networking/Capability Development)

Maj. Charlie Lewis  
(Military Operations/Training/Doctrine)

Lt. Col. Robert J. Ross, Ph.D.  
(Information Warfare)

Lt. Col. Nathaniel D. Bastian, Ph.D.  
(Advanced Analytics/Data Science)

Dr. Fernando Maymi  
(Cyber Curricula/Autonomous Platforms)

Dr. Paulo Shakarian  
(Social Threat Intelligence/Cyber Modeling)

Dr. David Gioe  
(History/Intelligence Community)

Dr. William Clay Moody  
(Software Development)

Dr. David Thomson  
(Cryptographic Processes/Information Theory)

Dr. Dawn Dunkerley Goss  
(Cybersecurity Optimization/Operationalization)

Dr. Jeffrey Morris  
(Quantum Information/Talent Management)

Dr. Robert Thomson  
(Learning Algorithms/Computational Modeling)

Dr. Michael Grimaila  
(Systems Engineering/Information Assurance)

Ms. Elizabeth Oren  
(Cultural Studies)

Lt. Col. (P) Natalie Vanatta, Ph.D.  
(Theatcasting/Encryption)

Dr. Steve Henderson  
(Data Mining/Machine Learning)

Lt. Col. Mark Visger, J.D.  
(Cyber Law)

### EDITORIAL BOARD

Dr. Andrew O. Hall, (Chair.)  
Marymount University

Dr. Martin Libicki  
U.S. Naval Academy

Dr. Bhavani Thuraisingham  
The University of Texas at Dallas

Dr. Amy Apon  
Clemson University

Dr. Michele L. Malvesti  
University of Texas at Austin

Ms. Liis Vihul  
Cyber Law International

Dr. David Brumley  
Carnegie Mellon University

Dr. Milton Mueller  
Georgia Tech School of Public Policy

Prof. Tim Watson  
University of Warwick, UK

Col. (Ret.) W. Michael Guillot  
Air University

Col. Suzanne Nielsen, Ph.D.  
U.S. Military Academy

Prof. Samuel White  
Army War College

Dr. Hy S. Rothstein  
Naval Postgraduate School

### CREATIVE DIRECTORS

Sergio Analco | Gina Daschbach

### LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

### PUBLIC AFFAIRS OFFICER

Maj. Joseph Littell

### KEY CONTRIBUTORS

Clare Blackmon  
Nataliya Brantly

Kate Brown  
Erik Dean

Debra Giannetto  
Carmen Gordon

Col. Michael Jackson  
Lance Latimer

Charles Leonard  
Alfred Pacenza

Michelle Marie Wallace

### 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](http://mc04.manuscriptcentral.com/cyberdr)

### WEBSITE

[cyberdefensereview.army.mil](http://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.

© U.S. copyright protection is not available for works of the United States Government. However, the authors of specific content published in The Cyber Defense Review retain copyright to their individual works, so long as those works were not written by United States Government personnel (military or civilian) as part of their official duties. Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.

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.





---

**AN OFFENSIVE FUTURE?**

GUEST EDITORS

**Dr. Andrew C. Dwyer and Dr. Amy Ertan**

---

INTRODUCTION

<b>Dr. Andrew C. Dwyer</b> <b>Dr. Amy Ertan</b>	9	An Offensive Future?
----------------------------------------------------	---	----------------------

---

SPECIAL EDITION ARTICLES

<b>Alicia Bates</b>	17	Prepare and Prevent, Don't Repair and Repent: The Role of Reinsurance in Offensive Cyber
<b>Matthias Dellago</b> <b>Daniel W. Woods</b> <b>Andrew Simpson</b>	31	Exploit Brokers and Offensive Cyber Operations
<b>Dr. Bryan Nakayama</b>	49	Democracies and the Future of Offensive (Cyber-Enabled) Information Operations
<b>Ewan Lawson</b>	67	Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations
<b>Dr. Nori Katagiri</b>	79	Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations
<b>Dr. Brandon Valeriano</b>	91	The Failure of the Offense/Defense Balance in Cyber Security
<b>Dr. Joe Burton</b>	103	The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity
<b>Dr. Rod Thornton</b> <b>Dr. Marina Miron</b>	117	Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking

---



# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆



# Introduction: An Offensive Future?

---

Dr. Andrew C. Dwyer

Dr. Amy Ertan

The recent cyberattacks against Colonial Pipeline and Solar Winds in the United States, the Health Service Executive in Ireland, and extensive and ongoing cyber activity in Ukraine highlight the continuing threats and complex security needs of our interdependent societies. Such operations and attacks are conducted by states that do not claim to possess offensive cyber capabilities, such as Russia and China, or by sophisticated cybercriminal gangs who commonly deploy ransomware, particularly with “hack and leak” operations, to generate an enormous amount of revenue. In response, many states have developed cyber capabilities to address the growing insecurity of states, their citizens, and various communities, with varying degrees of success and organization.<sup>1</sup> Thus, as states have been establishing more assertive responses to malicious cyber activities through offensive cyber forces or units of their own, there has been a concurrent development of connecting this with broader cyber security, resilience, and capacity building, often around the pursuit and projection of cyber power.

In this special issue of *The Cyber Defense Review*, the contributing authors were asked to explore the contours of living in a future world where there is more explicit activity, and public recognition of, offensive cyber operations and the key issues that need to

© 2022 Dr. Andrew C. Dwyer, Dr. Amy Ertan

<sup>1</sup> Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: C Hurst & Co Publishers Ltd, 2022), and for a discussion on the UK, see Joe Devanny et al., “The National Cyber Force That Britain Needs?” (London: King’s College London, April 21, 2021), <https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf>.



**Dr. Andrew C. Dwyer** is an Addison Wheeler Research Fellow at Durham University (Durham, UK) in its Department of Geography. His research covers technological decision-making, offensive cyber policy, as well as creative approaches to the study of cybersecurity. He is Co-Lead of the Offensive Cyber Working Group and in Fall 2022 will be an Assistant Professor in the Information Security Group at Royal Holloway, University of London.

be considered. Such a process suggests that the need for attentiveness is not only limited to military and strategic spheres and recognizes that cybersecurity and cyber power must be maturely and appropriately understood. Offensive cyber operations must consider social, cultural, political, and economic interests together with civil society, private businesses, and academia, which some states call a whole-of-society approach. Thus far, there has been a limited analytical focus on such a critical and broad interpretation of offensive cyber activities, which this special issue seeks to address. By considering what an “offensive future” may look like, as guest editors, we do not define offensive cyber nor take a position on its future use as different communities will interpret this differently. We instead note that offensive cyber activities are already part of our present and have developed considerably upon older practices of intelligence and effects operations, as much as their effects are felt unevenly. Therefore, we present a set of thought-provoking articles examining this nascent discussion, with its contested definitions and contours, and offer insights into numerous practices and implications across three primary themes.

In the first theme, there is an exploration of some of the economics that underpin both the capacity to engage in offensive cyber operations through an analysis of exploits as well as the implications for societies that may be the target of such actions. Kicking off the special issue, in “Prepare and Prevent, Don’t Repair and Repent: The Role of Reinsurance in Offensive Cyber,” Alicia Bates explores the power of resilience and argues for the need for a new framework of cyber insurance that accounts for offensive cyber activity. In so doing, the paper argues that a reinsurance framework may reduce the risks and unintended consequences of offensive cyber operations and thus a state’s capac-



**Dr. Amy Ertan** is a cybersecurity fellow at the Harvard's Belfer Center for Science and International Affairs, cyber strategy researcher at the NATO Cooperative Cyber Defence Centre of Excellence. She received an Information Security doctoral degree from Royal Holloway, University of London. Her research focuses on cyber conflict and the security implications of emerging technology, and she is the co-lead of the Offensive Cyber Working Group. Amy's recent co-authored publications include the NATO CCDCOE report: "Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment" and the *King's Policy Institute Report*: "The National Cyber Force that Britain Needs?" She holds CIS-SP and CRTIA qualifications and has previously worked in cyber-wargame scenario design, human factors cyber security research and strategic cyber intelligence.

ity to deliver an offensive strategy that can receive a more positive reception from its publics. In exploring the technical capabilities of conducting operations, Matthias Dellago, Dr. Daniel Woods, and Dr. Andrew Simpson examine broker quotes for cyber exploits from those who claim to sell to government actors in "Exploit Brokers and Offensive Cyber." Their analysis informs our understanding of supply and demand for offensive cyber capabilities in private markets, and the transforming economies of exploits.

In a second theme, authors paid attention to how offensive cyber is organized, approached, and constructed. During a time when there are different, competing visions of the future of the Internet, in "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," Dr. Bryan Nakayama analyzes how Western democracies have responded to cyber-enabled information operations, and concludes that democracies should avoid practicing such offensive operations entirely in an alternative perspective on what our future should be. Moving to a focus on organizations, in "Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations," Dr. Ewan Lawson carefully details how the organizational context in which offensive cyber capabilities operate are blurred between intelligence agencies and the military. This research argues that such a blurring is problematic as it both contributes to unintended escalation between states and increasing the potential for destructive "grey zone" activity below the threshold of war, with implications for the application of international humanitarian law (IHL). Dr. Nori Katagiri continues this conversation by examining when the conduct offensive cyber operations is an appropriate and required course of action, and proposes a set of criteria in "Three Conditions

for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations,” alongside detail on associated challenges in meeting each of the proposed conditions.

After exploring economics, organization, and construction, the third theme of this special issue offers two pervasive perspectives on the narratives and assumptions on offensive cyber activity. In “The Failure of Offense/Defense Balance in Cyber Security,” Dr. Brandon Valeriano highlights the pitfalls in the attempts to apply the principle of an offense/defense balance to research. In so doing, he identifies a “strategic malaise” resulting from a mistaken approach in assuming that the advantage always lies with the attacker. In comparison, Dr. Joe Burton explores the diverse academic approaches to cyber conflict in “The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity,” which highlights the power of interdisciplinary scholarship to enable more holistic and nuanced debates and understandings of the field’s dynamics. He draws from International Relations, Political Psychology, International Law, and Computer Science to explore the intricacies, mistranslations, emphases and contributions of each.

Dr. Rod Thornton and Dr. Marina Miron then close out the issue as they explore how Russia thinks through the power of cyber capabilities and their potential to generate strategic outcomes in “Winning future wars: Russian offensive cyber and its vital importance in Moscow’s strategic thinking.” This is demonstrative of a broader approach to strategic thinking where the country sees itself at a strategic disadvantage to NATO in other arenas of warfare. Both authors also offer some early reflections in relation to the ongoing war in Ukraine, demonstrating some of the differences between Western and non-Western conceptualizations of offensive cyber in the 21<sup>st</sup> Century.

We hope that these papers—variously covering economics, organization, strategy, and the case of Russia—offer avenues to broaden the scope of discussion on offensive cyber activity and its interdependencies with cyber security and cyber power. Each paper adds something new to the discussion, helping to address the urgent need for more nuance in this space. There is, however, a need for further debate that goes well beyond the scope and generosity of these eight papers. This debate ought to explore emerging and disruptive technological trends, examine international relationships beyond the usual suspects of “great” power competition between the US, China, and Russia as well as the role of “second-tier” powers including the UK and France. Similarly, conversations must take place at all levels, from exploring organizational contexts to clarifying processes around oversight and talent, to discussions on international norms and deterrence theory. While this special issue explores several of these themes, efforts to disentangle these themes and subjects are needed more than ever. We therefore see this as an open invitation to deepen and extend the conversation. The Offensive Cyber Working Group—which we co-lead and under which these papers were curated—will continue to promote conversations on these themes and welcomes engagement from research and policy communities to do so.

Finally, we thank all the contributing authors for their time and expertise for this issue. We are particularly grateful to Dr. Corvin Connolly and the editorial team at *The Cyber Defense Review*, who have been incredibly supportive throughout the entire publication process. It has been a pleasure.♥



# THE CYBER DEFENSE REVIEW

◆ SPECIAL EDITION ARTICLES ◆



# Prepare and Prevent, Don't Repair and Repent

*The Role of Reinsurance in Offensive Cyber*

---

Alicia Bates

## ABSTRACT

*Insurance is often treated purely as a tool to mitigate financial risk. The insured can pay a premium for the confidence that if a cyber-attack occurs, they are indemnified for their losses. This paper advocates that insurance can play a more significant role dealing with offensive cyber, by way of relying upon a reinsurance framework. An appropriate insurance framework which assists a non-state actor before, during, and after an attack can facilitate a coordinated response to supporting a state's national security objectives. When a state opts to use an offensive cyber operation, there is a risk that the operation will inflict unintended consequences/harms and will trigger a retaliatory attack. The proposed reinsurance framework would assist in improving a business's resilience and security. An underlying reinsurance regime will ensure the framework transfers risk from a specific business and spreads it across society. This paper argues that by reducing and responding to risks and unintended consequences of offensive cyber operations with reinsurance, a state's offensive cyber strategy may receive a more favourable reception from society. This reduces the risk that an offensive cyber strategy may delegitimise the state.*

## INTRODUCTION

**D**efensive cyber operations have traditionally dominated state responses to attacks upon domestic-based networks.<sup>[1]</sup> However, there is an increasing shift towards states choosing to use offensive cyber operations against other states and non-state actors.<sup>[2]</sup> While a set definition does not exist in the literature, offensive cyber strategies could involve a state “pursuing or disrupting cybercrime, conducting digital counterintelligence, or military cyber operations.”<sup>[3]</sup> The trend of favouring offensive



**Alicia Bates** is a Senior Tutor at the University of Law where she teaches international commercial law. Alicia is currently studying for her Ph.D. at King's College London under the supervision of Professor Özlem Gurses and Dr. Tim Stevens. Her Ph.D. is entitled: 'Terrorism: when, not if. Time to insure the uninsurable risk? *An intensive investigation into the legal framework governing mandatory insurance.*' Alicia's research interests lie in insurance, terrorism, and cyber. Prior to undertaking her Ph.D., Alicia was called to the Bar of England and Wales by the Honourable Society of the Middle Temple where she was awarded the Harmsworth Scholarship and the Hong Kong Scholarship. Alicia has also taught at BPP University and taught insurance law as a visiting lecturer at King's College London. Alicia is a Fellow of the Higher Education Academy.

cyber operations raises two issues for states. First, how should the state respond to the risk that foreign states might use an offensive cyber strategy against them or domestic non-state actors? Second, what are the risks of a foreign state retaliating against a state that has deployed an offensive cyber strategy? The issue of attribution is concomitant with both of these questions. Offensive cyber operations are typically classified. This presents practical and legal issues of how a state, or insurer, investigates and attributes an attack.

When a state uses an offensive cyber strategy, there is a risk that the operation will result in a foreign state retaliating.<sup>[4]</sup> This retaliation could harm the state or non-state actors. This paper suggests that an insurance framework, which is underpinned by reinsurance, and assists a business before, during and after an attack, could improve the resilience and security of domestic businesses in response to cyber attacks. This increase in resilience and security, coupled with the spread of risk by way of reinsurance, would support a state's national security objectives when their strategy involves offensive cyber operations.

Insurance companies can enlist a cyber expert to assess a business's cyber security prior to the insurance contract being drafted. The insurer can impose contractual obligations upon the insured to ensure that some or all of the expert's recommendations to improve their cyber security are implemented before the commencement of the insurance policy. This contractual protection mitigates the insurer's scope for liability. Insurance companies could hire a team of cyber experts who are on-hand to assist an insured during an attack. Having immediate help will limit the impact of the attack. This is not only beneficial to the insured, who will be more likely to experience fewer losses, but also the insurer who will, consequently, have to pay out less to the insured.

The author anticipates the insurance industry would not receive her proposals favourably unless an adequate state-based reinsurance framework underpinned the proposals. State-based reinsurance would assist insurance companies meet their liabilities to the insured once a claim was over a certain financial amount.<sup>[5]</sup> This would ensure that insurers were able to withstand the potential implications of a state's offensive cyber operations. Reinsurance would spread the risk of a cyberattack across society. The transfer and spread of risk from an insured business to society as a whole, will provide greater flexibility for the deployment of a state's national security objectives. The mitigation of loss arising from an insurer's assistance in improving resilience and security prior, during and after attack is important to ensure the underpinning reinsurance regime remains financially viable. The pre-emptive establishment of reinsurance, underpinned by a state guarantee, allows a state to acknowledge that their strategies may cause direct or indirect harm to domestic non-state actors.

While this paper addresses reinsurance in the UK, it is important to note that the ideas in this paper could easily be extrapolated and relied upon by many states across the globe, such as the US. The idea in the paper could see a broader move by states to support the resilience of domestic companies through reinsurance. This could improve perceptions of a state's offensive cyber strategies. This proposed insurance framework may appear to be defensive in nature and to some extent it is. However, insurance can enable a good defence against offensive cyber strategies. By improving this defence, it supports a state's national security objectives.

### ***Part I: The Scope for Harm Emanating from Offensive Cyber Strategies***

Insurance is a risk management tool.<sup>[6]</sup> Insurance contractually divides a specific risk between the policy holder (the insured) and an insurance company (the insurer). In recent years, the market has pushed for indemnity insurance to be offered to cover cyber-attacks. The WannaCry cyber-attack exemplifies why insurance is sought by the market. Within 24 hours, 230,000 computers in around 150 countries had been affected.<sup>[7]</sup> This affected governmental organisations and businesses alike. The National Health Service (NHS) saw a third of trusts across the UK affected because of infected and locked out devices and consequential cancelled appointments.<sup>[8]</sup> Beyond the practical impact, WannaCry also had a fiscal impact on the NHS. Kristensen et al found that “[t]he total economic value of the lower activity at the infected trusts during this time was £5.9m including £4m in lost inpatient admissions, £0.6m from lost A&E activity, and £1.3m from cancelled outpatient appointments.”<sup>[9]</sup> Had a kill switch not been found on the same day as the WannaCry attack, one can foresee how these losses could have been greater. It is estimated that if the attack had affected all trusts, the loss in activity alone could have reached up to £35m.<sup>[10]</sup> While this attack was not a target arising from the UK's offensive cyber operations, it is a clear example of how a foreign state's attack on part of the UK's critical infrastructure could cause considerable financial harm and disruption.

The attack on SolarWinds helps to further contextualise how cyber attacks can induce retaliatory attacks. SolarWinds is a US information technology firm which attracts high profile

clients such as Fortune 500 companies and government agencies.<sup>[11]</sup> In March 2020, SolarWinds sent updates of their software to 33,000 customers (around 18,000 customers installed the update). This update included a malicious code which allowed the hackers to access sensitive customer information and install malware to spy on customer systems. The level of sophistication of the attack meant that it went undetected for months and to date, many customers do not know if they were a victim of the attack.<sup>[12]</sup> It is believed that the malicious code was directed by the Russian intelligence service. The attack resulted in President Biden imposing sanctions against Russia. When deciding to employ these sanctions, President Biden will no doubt have been live to the possibility that Russia could retaliate. This raises the question of how can a state ensure that their domestic defence is able to withstand retaliatory effects from an offensive cyber strategy?

Beyond the fiscal impact of an attack arising from business interruption, an insured can face other losses; for example, the insured may become liable for breaches of confidentiality to third parties or a loss in reputation. The CEO of Lloyd's London, Inga Beale, argues that "[t]he reputational fallout from a cyber breach is what kills modern businesses. And in a world where the threat from cybercrime is when, not if, the idea of simply hoping it won't happen to you, isn't tenable."<sup>[13]</sup> This reputational impact can occur because an assailant can access a great deal of confidential information which, if leaked, could cause significant harm to many of the companies associated with the target company.

An example of this is the Hafnium attack on Microsoft. The Hafnium attack involved a group attributed as a Chinese state-sponsored actor. The group exploited vulnerabilities with Microsoft's Exchange Server. While estimates differ greatly, it is estimated that this attack impacted anywhere between 10,000 and 250,000 of Microsoft's customers, including businesses, governmental agencies, and schools.<sup>[14]</sup> It is possible that these customers will have developed negative perceptions of Microsoft as a result of the impact on Microsoft's Exchange software. This might have resulted in those customers looking to Microsoft's competitors for the provision of email software. This shift in customer behaviour would likely harm Microsoft's profit margins. However, beyond this, the Hafnium attack demonstrates that there are positive externalities for strong defence against cyber operations, an attack on one company can harm other actors, such as businesses within the supply chain of the target business. With relations between the US and China continually being challenged, the scope for either state to retaliate and use cyber offensive strategies in response to Hafnium is foreseeable.

The attacks cited highlight the level of risk that can be attributed to cyber-attacks. With the continuous evolution of technology and growing willingness of states to use offensive cyber capabilities, one might argue that the scope for harm transcending quantifiable losses could only continue to evolve. Thus, it is important to ask: how can reinsurance assist in allowing the role of insurance to evolve and move beyond simply indemnifying an insured's losses arising from an offensive cyber operation?<sup>[15]</sup>

## *Part II: Improving a Non-State Actor's Resilience Before an Attack*

The premium paid by the insured to the insurer represents the cost of the risk covered by the policy.<sup>[16]</sup> This is termed the “actuarially justified premium.”<sup>[17]</sup> If the premium is too low and a loss is realized, an insurer could become insolvent fulfilling its liability to the insured. Premiums are therefore set at a rate to create a sufficiently large capital to ensure considerable losses can be covered. While many economic models have been developed regarding cyber risk estimation and premiums,<sup>[18]</sup> it is worthwhile asking: what if this premium could cover a service beyond the promise of indemnifying future losses?

In English law, the insured must disclose any information which may affect the objective insurer's decision to insure. This disclosure will satisfy the insured's duty of fair presentation of the risk.<sup>[19]</sup> For example, the reasonably prudent insurer would likely want to know about a previously successful cyber-attack on the insured, as this would identify potential vulnerabilities in the insured's networks. However, the insured must only disclose information that they know or ought to know.<sup>[20]</sup> The difficulty is that many companies, understandably, lack knowledge about their cyber risk. This is prevalent in relation to risks emanating from offensive cyber operations as states rarely disclose the full detail of their operations for the purposes of national security. Thus, the disclosure obligations on the insured are fairly minimal; not least, because any information which is publicly available regarding the threat actor need not be disclosed by the insured to the insurer, as the insurer can be presumed to know the information.<sup>[21]</sup>

Cyber experts can assist companies in assessing and minimising their risk. While cyber experts are not going to be privy to a state's offensive cyber strategies, they will have an in-depth understanding of vulnerabilities with specific software and industries. However, these experts are expensive, and the cost is rising. In 2012, Caldwell Partners, an Executive Search Firm, paid \$650,000 a year for a cyber expert to join on as Chief Information Security Officer. In 2019, that salary had risen to \$2.5 million.<sup>[22]</sup> Bloomberg accounts this growth to the increase and severity of cyber-attacks, and also the fear of litigation and the associated fines.<sup>[23]</sup> Whilst many advisory firms are available to conduct cyber risk assessments, these are costly, and the cost is not going to decrease soon. This might mean that the cost of an expert is considered by the insured to be unaffordable or disproportionate to the perceived benefit. One way an expert could be used would be by conducting a risk assessment of the insured's business prior to the insurance policy being drafted. This risk assessment could be accompanied with recommendations for improvements. Although one might perceive this as expecting the insurance industry to provide a new and free service to the insured, the insurance industry will actually see reduced claims as a result of the increased resilience. Furthermore, insurers do already assess a client's risk either at the point of quotation or renewal. This risk assessment dictates the premium the insured will pay. The proposal therefore seeks to use the wealth of knowledge that advisory firms have and input it into the insurance coverage process in a standardized manner.

Used appropriately, this risk assessment could mean that insurance could be seen as a vital tool to improve a company's resilience and improve standards overall to reduce the impact of cyber operations by states. The anticipated cover would compensate the insured for losses arising from a foreign state's cyber operations. A definition clause in the policy would dictate that the policy would cover operations which have been attributed to a state directly, or a stated sponsored actor, as seen with Hafnium. There would be no requirement that the attack was in retaliation to the domestic state's cyber operations; any legal clause attempting to do so, would render the policy challenging to claim on owing to evidential issues, not least with attribution. Many offensive cyber strategies are subject to national security. This confidentiality means that proving an attack was in retaliation could be near impossible. That is not to say that attributing the attack which has caused losses will be straightforward. Although attacks such as SolarWinds and Hafnium have been attributed to state-sponsored actors, this took a considerable amount of time. The issue of attribution will need to be explored further and is worthy of discussion with academics across the field. However, it is worthwhile noting that the legal standard of attribution and the political standard is very different. This leads the author to believe that attribution is not an insurmountable obstacle for the proposed policy. As a matter of law, an insurer is liable where the loss was caused by an insured peril. Causation and loss must be established on the balance of probabilities; in other words, the loss was more likely than not a result of a foreign state's cyber offensive operations. For many states, this would be too low of a bar to explicitly attribute an attack to another state. Often states are tentative in their attribution, as they are mindful of the potential ramifications if their attribution is proved to be inaccurate. Thus, upon overcoming the challenges faced with attribution, one can foresee how the coverage may reassure a state that they can use a cyber offensive strategy, safe in the knowledge that they have an adequate defense, should retaliation occur.

Cyber experts can reflect upon previous attacks to assess a company's vulnerabilities and develop a system of best practices while responding to the specific company in question. These recommendations would then be assessed by the insurer, who could then decide whether the proposed improvements should remain voluntary for the insured or whether they ought to be incorporated as clauses into the insurance policy. These clauses could take two forms: a warranty or a condition precedent.

A warranty is a promise that the insured has done something (a present warranty) or will continue to do or not do something (a continuing warranty).<sup>[24]</sup> A warranty might confirm that a state of affairs is true, for example, that the insured has installed a firewall onto their computer systems. If this warranty is breached, the insurer's liability is suspended for the period of time that the insured has not complied with the warranty.<sup>[25]</sup> It should be noted that, save that it is a risk defining term, this suspension will only relieve the insurer of liability if the risk of the specific loss faced by the insured was materially affected by the breach.<sup>[26]</sup> For example, a failure to install a firewall would be unlikely to materially affect the insured's risk of their premises

flooding. However, as we are speaking about losses arising from a cyber attack, one can assume that the imposed warranties would materially bear on the losses the insured was seeking to cover insofar as offensive cyber operations are concerned and therefore might be regarded as a risk defining term. The scope for loss arising from a cyber attack would likely mean that most insureds would be motivated to ensure that they would be indemnified under the policy.

Alternatively, the insurer could impose a condition precedent on the insured. There are three types of condition precedent: to the policy, to the inception of the risk, and to the liability. A condition precedent to the liability is relevant to the claims making stage. A condition precedent to the policy means that the validity of the entire contract depends upon the insured's compliance with the condition precedent. Furthermore, a condition precedent to the inception of the risk means that while a contract exists between the insurer and the insured, there is no coverage of the risk unless there is compliance—in every practical sense, the contract is useless without compliance with the term. If the insurer is particularly interested in the insured taking specific steps prior to agreeing to indemnify the insured, these options would be more desirable for the insurer. An example might be that the insurer stipulates that an insured imposes a multi-factor authentication on all technological devices for all users. In this scenario, a condition precedent to the policy would mean that the policy would not be rendered valid until the authentication system was employed. Alternatively, a condition precedent to the inception of the risk would mean that, while the policy was valid, it would not cover the risk of cyber-attacks until the authentication system was active.

In summary, the insurer can provide a cyber expert to the insured as part of the insurance policy package. The cyber expert can identify the insured's vulnerabilities, which will then allow the insured to take proactive steps to minimize their risk and improve their resilience. The insurer can enhance this protection by including terms that require the insured to take the necessary steps to minimise their risk of loss. The insurer would be able to factor the inclusion of these clauses into their risk assessment, known in the insurance industry as the underwriting process.

### ***Part III: Improving a Non-State Actor's Resilience and Security During and After a Cyber Attack***

While the insured's risk can be mitigated by way of improving their resilience, one must accept that the risk a non-state actor will be harmed because of an offensive cyber strategy (be it indirectly or directly) cannot be eradicated. Because of this, it is pertinent to reflect upon how an insurer can assist the insured in ensuring that the losses arising from a cyber-attack are constrained as much as possible. This is a laudable goal. If the UK plans to use offensive cyber strategies, improving non-state actors' defences against a foreign non-state actor's retaliatory attack recognizes the potential consequences of the UK's actions. This is not only important for improving a non-state actor's resilience prior to an attack, but also their resilience and security during and after an attack. If state and non-state actors within the UK have a more robust defense

system and if the UK is forced to take a particularly extreme offensive cyber operation (such as disrupting the supply of a utility like electricity to an entire city or engaging in military conflict), the state and non-state actors within the UK will feel more confident in defending any retaliatory attacks. By using the proposed framework, the UK further demonstrates that its offensive cyber strategies are being used in a manner which is compatible with democratic governance.

One way to improve democratic governance is by ensuring there is accountability, oversight, and transparency within the government.<sup>[27]</sup> Oversight and transparency are not always achievable given the national security implications, the complexity of the associated networks and the associated expertise of oversight bodies, and the interplay between public and private cooperation.<sup>[28]</sup> In this regard, a focus upon accountability might facilitate the UK's use of offensive cyber strategies. As such, insurance could play an invaluable role in ensuring that any harm inadvertently imposed upon a non-state actor because of an offensive cyber strategy was compensated for accordingly. This is supported by Weber's approach towards the ethics of responsibility which suggests that a government should be mindful of pursuing a strategy which in the best interests of the nation.<sup>[29]</sup> While offensive cyber strategies may be entirely justified when someone is armed with the full information regarding the threat faced by the UK,<sup>[30]</sup> the government does still need sufficient support from society (who will likely be unaware of the extent of the threat) to ensure that their actions do not undermine the legitimacy of the government. The transfer and spreading of risk is one way insurance can assist in this regard. However, it is anticipated that the insurance industry would not view these proposals as favourable unless an adequate state-based reinsurance framework underpinned the proposals.

When the insurer has a team of cyber experts on hand, they can deploy the experts to the insured's premises as soon as they are notified that an attack is underway. This will particularly assist an insured who is victim of a retaliatory attack after a foreign state has engaged in offensive cyber strategy. It may be challenging to determine that the attack was as a result of an offensive cyber strategy at the point the insured realises an attack is taking place. This is not insurmountable. The insured will likely have multiple policies with the insurer which cover different types of risk. One policy may cover cyber attacks conducted by non-state actors, where the other covers state actors or state sponsored actors. This may be done under one comprehensive policy or under two separate insurance contracts. This article focuses upon offensive cyber and thus, further exploration of insurance cover must be limited. The author has produced research which considers how these policies can be used for cyber attacks more generally, and potentially for cyber terrorism, should it eventualise in the future. This highlights the potential scope for these policies to reshape the vast sectors of the insurance industry.

A cyber expert would be able to assist the insured in minimizing the harm and recovering from an attack as quickly as possible. We can consider the Hafnium attack on Microsoft as an example of how this could work in practice. The vulnerabilities in the software that led to the 0-day exploit have since been patched by Microsoft, but that software is used by many compa-

nies around the world. Cyber experts would be able to suggest how to address evolving threats by relying upon their knowledge developed from previous attacks in a way in which many non-state actors would be unable to do on their own.

Relying on a cyber-expert to assist would align with Woods and Böhme's research, which found current market practice dictates that when a policy holder suffers an incident, they call a hotline which puts together a team of responders to help the insured respond to the attack and minimize harm.<sup>[31]</sup> At the moment, insurers typically advertise a list of preferred or pre-approved cyber experts, having cyber experts on hand who could be deployed directly by the insurer as part of their insurance service would streamline the efficacy of the intervention.

To ensure the probability of successful intervention is as high as possible, the insured may consider introducing a condition precedent to the liability in the insurance policy. A condition precedent to the liability means that the insurer faces no liability unless the insured complies with the condition precedent at the claims making stage. For example, a condition precedent to the liability might require the insured to co-operate with the insurer in the period after the attack to ascertain the identity of the assailant. In the words of Longmore LJ in *Royal & Sun Alliance Insurance Plc v Dornoch Ltd*,<sup>[32]</sup> "a condition precedent to the liability of the reinsurer operates as an exemption to that prima facie liability."<sup>[33]</sup> If the insured failed to comply with the condition precedent and brings a claim for a loss, the claim will fail.<sup>[34]</sup> Thus, the insurer may wish to implement a claim provision which is a condition precedent to the liability and which stipulates that the insured must notify the insurer as soon as reasonably practical that an attack is underway. The insured could go further and introduce a time bar. For example, they could stipulate that the insured must notify the insurer within 3 hours of discovering the attack. The effect of failure to comply with such a condition precedent would mean that the insurer would not be liable for any losses arising from that specific cyber-attack.

It should be noted that a breach of this condition precedent does not invalidate the insurance policy and the insurer would remain liable for future claims, provided the insured complied with the clause on that occasion. This clause would also be important to safeguarding over-reliance upon a reinsurance regime. While the reinsurance regime further assists in developing state accountability, it is important that the regime remains fiscally viable. One way to ensure the reinsurance regime remains affordable is to mitigate the regime's use as far as possible.

#### ***Part IV: The Use of Reinsurance to Assist in Improving Domestic Resilience***

Whilst the above discussion has highlighted how insurance companies can facilitate improving the defensive position of non-state actors in the UK, thereby supporting the UK's national security objectives, it is important to ensure this framework is financially viable for insurers. To do this, it is important to briefly consider how state-based reinsurance could supplement the framework. This paper argues that reinsurance would indicate a state's willingness to support insurance companies in improving domestic resilience. This is because state-based reinsurance

could assist insurers where large sums were owed to non-state actors because of losses directly or indirectly emanating from the UK's offensive cyber operations.<sup>[35]</sup>

Insurance companies are businesses, therefore, while their service is to indemnify an insured's loss, upon an insured peril occurring, it is vital that the service provided is sustainable for the insurer. If a proposed service becomes financially unviable for the insurer, the insured's risk increases further as there is a chance that the insurer will become insolvent before indemnifying the insured. This would be problematic not only for the insurer and the insured but society as a whole, as a result of systemic risk: businesses are heavily interconnected and if one goes insolvent, there could be a ricochet effect which destabilizes the economy of a state. It can be argued that attacks such as WannaCry and Hafnium both demonstrate that cyber attacks can not only result in particularly high financial claims but also that minimizing the harm caused by cyber attacks positively impacts society as a whole. This is particularly true if we consider the fact that insurers typically insure a vast array of risks. Therefore, their insolvency would not only impact businesses but anyone who held an insurance policy with that insurer. If the UK is planning to employ further offensive cyber operations, it is worthwhile to reflect upon the impact that will have on non-state actors and their insurers. This is where reinsurance comes in and acts as a facilitator to improve domestic resilience throughout the UK.

Reinsurance is where the government provides an insurance framework to insurers. While the UK has Pool Re as a reinsurance scheme available for terrorism, no such reinsurance scheme exists for cyber risk. Pool Re was established, in tandem with the insurance industry and Her Majesty's Treasury, to help insurance companies offer insurance coverage after a terrorist attack. Pool Re provides reinsurance in the event an insurer is unable to meet the claims after an attack. Rather than allow for a situation where the insurance market rejects policies for cyber risk, it would be more appropriate for the government to pre-empt this development as part of their National Resilience Strategy, supported by the National Cyber Security Centre. Thus, the pro-active approach would likely increase societal perceptions of the UK's offensive cyber strategy as it is indicative of not only governmental accountability, but also the forward looking nature of the UK's offensive cyber strategy.

One might raise the question why reinsurance alone would not be sufficient to support the existing cyber insurance framework. As previously stated, an insurer's liability can be reduced by minimizing a non-state actor's scope for harm by improving their resilience and security. This is important if one accepts the proposition that a state's increased use of offensive cyber strategies is likely to, in turn, increase non-state actors' risk of attack by a foreign state. By using the proposed insurance framework in tandem with a reinsurance framework, it ensures any reinsurance provided by the government remains viable long term. For example, reinsurance might only be available to the insurer once their liability exceeds a certain financial sum. While it remains prudent for the insurer to invest some of the premium received by the insured into hiring the most skilled cyber security experts to minimize their scope for liability,

it could be required that an insurer be able to benefit from the reinsurance scheme. This would ensure that a middle ground is found between state accountability and a realistically affordable framework.

## **CONCLUSION**

As states continue to move towards using cyber offensive strategies, it is important to recognize the impact these strategies can have upon non-state actors. There are two points to consider in relation to the role of reinsurance with regards to offensive cyber operations.

First, by recognising the global trend towards states preferring offensive cyber strategies, it is important for the UK (and states across the globe) to improve their own defenses against a foreign state's use of offensive cyber operations. In this regard, insurers can transcend their classic indemnification role and evolve to providing a service that helps to prevent and mitigate the harm emanating from offensive cyber strategies thereby playing a key role in improving a non-state actor's security and resilience.

Second, when the UK uses an offensive cyber strategy, non-state actors can be indirectly and unintentionally harmed, not least if they become victim to retaliatory attacks. In this regard, a reinsurance framework, which spreads the risk from non-state actors across society will likely align with the UK's national security objectives. While a reinsurance regime plays an essential role in ensuring that the proposed framework is feasible for insurers, it is essential that the reinsurance regime is equally feasible long term. For this reason, it is important that insurance work towards improving the insured's resilience using pre-emptive cyber advice and integrating this into contractual obligations for the insured.🛡️

## NOTES

1. S Bradbury, "The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal* 2, no. 2 (2011).
2. For example, the UK was the first to acknowledge that offensive cyber was a viable option, within the confines of international law, to respond to the risk of a cyber-attack see J Blitz, "UK becomes first state to admit to offensive cyber attack capability," *Financial Times*. 2013, <https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de>. Furthermore, the creation of the National Cyber Force in 2021 was intended to improve the UK's offensive cyber capabilities see "National Cyber Strategy 2022," UK Government, 2022, accessed 17th February, 2022, <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>.
3. *The National Cyber Force that Britain Needs?* (Kings College London; Offensive Cyber Working Group, April 2021).
4. Although retaliation is not strictly permissible under Article 51 of the UN Charter, this does not mean that offensive cyber strategies cannot enter a grey area where the line between legitimate proportionate responses and unlawful retaliatory responses blur.
5. This financial amount would be determined by the state.
6. F Martin, *The History of Lloyd's and of Marine Insurance in Great Britain* (London: The Lawbook Exchange Ltd, 1876).
7. "Cyber-attack: Europol says it was unprecedented in scale," *BBC News* May 13, 2017, <https://www.bbc.co.uk/news/world-europe-39907965>.
8. W Smart, "Lessons learned review of the WannaCry Ransomware Cyber Attack," February 1, 2018.
9. S Kristensen, S Ghafur, K Honeyford, G Martin, A Darzi and P Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *npj Digital Medicine* 98, no. 12 (2019).
10. *Ibid.*
11. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal," *Business Insider*, 2021, <https://www.businessinsider.com/solar-winds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T>.
12. D Volz and R McMillan, "Hack Suggests New Scope, Sophistication for Cyberattacks," 2020, <https://www.wsj.com/articles/hack-suggests-new-scope-sophistication-for-cyberattacks-11608251360>; "The SolarWinds Cyber-Attack: What You Need to Know," 2021, accessed March 15, 2022, <https://www.cisecurity.org/solarwinds>.
13. "Closing the gap. Insuring your business against evolving cyber threats," 2017, accessed 30th October 2021, <https://assets.lloyds.com/assets/pdf-lloyds-cyber-closing-the-gap-full-report-final/1/pdf-lloyds-cyber-closing-the-gap-full-report-final.pdf>.
14. R McMillan and D Volz, "China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers," *The Wall Street Journal* 2021, [https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991?mod=tech\\_lead\\_pos1](https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991?mod=tech_lead_pos1).
15. It should be noted that some insurers may already play a role in improving a business' security and resilience. For example, insurers may pay for the expenses incurred to prevent or minimise the insured loss. The insured might prevent a loss and might claim the expenses incurred for that purpose from the insurer. Moreover, insurers generally ask the assured to take risk mitigation precautions. As such, whilst the proposals in Part II and III demonstrate how the insurance industry might move their collective practices to assist offensive cyber operations, the main focus of this paper is on how a state-based reinsurance scheme can help develop the insurance industry's facilitation of improving domestic defence in anticipation of a retaliatory attack after an offensive cyber strategy.
16. F Ewald, "Risk in Contemporary Society," *Connecticut Insurance Law Journal* 6 (2000).
17. *Ibid.*, 395.
18. Y Miaoui and N Boudriga, "Enterprise security economics: A self-defense versus cyber-insurance dilemma," *Wiley* 35 (2019).
19. Insurance Act 2015, s.3.
20. *Ibid.*, s.3(4).
21. *Ibid.*, s.3(5)(d).

## NOTES

22. "Cybersecurity Pros Name Their Price as Hacker Attacks Swell," Bloomberg, 2019, accessed 31st October 2021, <https://www.bloomberg.com/news/articles/2019-08-07/cybersecurity-pros-name-their-price-as-hacker-attacks-multiply>.
23. Ibid.
24. Marine Insurance Act 1906, s.33(1).
25. Insurance Act 2015, s.10.
26. Ibid, s.11.
27. *Democratic Governance Challenges of Cyber Security*, (DCAF Horizon, 2015).
28. *ibid*.
29. M Weber. *The Profession and Vocation of Politics. In Political Writings* (Cambridge: Cambridge University Press 2000). 309-369.
30. As explored in Martin. *Short Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age*.
31. D Woods and R Bohme, "How Cyber Insurance Shapes Incident Response: A Mixed Methods Study," *The 20<sup>th</sup> Workshop on the Economics of Information Security* (2021), <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-woods.pdf>.
32. [2005] Lloyd's Rep I.R 544, para 19.
33. *Ibid*.
34. As this type of clause falls outside of the scope of s.11 of the Insurance Act 2015 this would not be a hindrance for the insurer who wants to be relieved from the liability for the assured's breach of this term.
35. How insurance would define offensive cyber operations for this purpose is worth further exploring in future academic writing. Similarly, clear rules would need to be established setting out when the reinsurance could be relied upon by insurers.



# Exploit Brokers and Offensive Cyber Operations

---

Matthias Dellago  
Andrew C. Simpson  
Daniel W. Woods

## ABSTRACT

*A necessary step in conducting offensive cyber operations is developing or acquiring an exploit, i.e., a means for taking advantage of a software vulnerability or security deficiency. While these can be developed within government agencies, they can also be procured from private actors. Studying these private markets present an opportunity to understand offensive cyber operations, especially as markets break from the secretive culture of intelligence agencies. This article provides novel evidence of such opportunities by collecting data in the form of the prices quoted by an exploit broker who claims to sell to governments. We find exploit price inflation of 44% per annum, and higher prices for exploits targeting mobile devices relative to desktop devices. Exploits requiring additional capabilities like physical access to the device are quoted at a discount, and no-click remote access vulnerabilities carry a heavy premium. The broker does not quote prices for any exploits that specifically target industrial control systems or IoT devices. We conclude by discussing how these results inform the future of offensive cyber.*

## INTRODUCTION

The emergence of offensive cyber operations (OCO) – “the adversarial manipulation of digital services or networks”<sup>[1]</sup> – creates new considerations in military strategy and government policy. The resulting debates consider issues like the nature of cyber weapons,<sup>[2,3]</sup> the possibility of cyber war<sup>[4,5]</sup> the role of norms of responsible behavior<sup>[6,7]</sup> and, most importantly for this paper, the role of private actors in developing and deploying offensive cyber technology.<sup>[8,9]</sup> Such issues are even spilling over into the public sphere as evidenced by Nicole Perlroth's New York Times bestseller<sup>[10]</sup> arguing that

© 2022 Matthias Dellago, Andrew C. Simpson, Daniel W. Woods



**Matthias Dellago** is a computer science master's student at the University of Innsbruck. He earned his bachelor's degree in physics from the University of Vienna. His research interests include security and privacy, especially from an economic perspective.



**Andrew Simpson** holds a BSc in Computer Science from Swansea University and an MSc and a DPhil from the University of Oxford. He is currently an Associate Professor in Software Engineering in the Department of Computer Science at the University of Oxford.

private actors who supply offensive cyber technology are facilitating repressive regimes in targeting opposition politicians and journalists.

To incorporate such actors into national cyber strategy and to ensure responsible behavior,<sup>[11]</sup> it is important first to understand the market structures through which they operate. We apply the tools of security economics<sup>[12]</sup> to understand the business processes and price structure surrounding the supply of offensive cyber technology. Doing so provides a rare opportunity to collect empirical data on offensive cyber operations, as such private actors break from the secretive culture of intelligence agencies. While prior work has focused on bug bounty programs<sup>[13]</sup> and illegal underground forums,<sup>[14]</sup> we provide a longitudinal analysis of a zero-day exploit broker whose customers are “government organizations (mainly from Europe and North America).”<sup>[15]</sup> Our empirical results show that the mean exploit price is increasing by \$234 per day or 44% per annum. Exploits of both Apple operating systems and mobile devices have a higher average price in our dataset. In terms of the application targeted, exploits targeting communications (e.g., emails and messengers) have the highest average price. Further, we found no evidence that this broker procures exploits of technologies specifically targeting industrial control systems. These findings may not generalize beyond the idiosyncratic broker we study, especially given prices are based on the maximum price advertised for each exploit rather than actual payouts.

Turning to the question of this CDR Special Edition, these insights can inform the future of offensive cyber. First, exploit price inflation represents a growing constraint on offensive operations. Importantly, this constraint binds ex-ante unlike imposing costs via deterrence. Increased rewards for exploits in private markets function to increase the staffing costs for states maintaining internal offensive cyber capabilities and may motivate export controls and other policy interventions.



**Daniel Woods** is a Lecturer in Cybersecurity at the University of Edinburgh. His post is jointly appointed by the British University in Dubai. He received his Ph.D. in Cybersecurity from the University of Oxford's Computer Science Department.

## RELATED WORK

Selling exploits to a broker is but one of many ways for an independent security researcher to share information. The options available include:<sup>[16]</sup> privately reporting the information to the vendor (possibly in exchange for a bug bounty) or to a legitimate third party; selling the information on the black market; and sharing the information publicly. Before we turn to economic incentives, it is worth noting that many researchers share information without any financial reward. For example, the CERT Coordination Center (CERT/CC) have been running coordinated vulnerability disclosure for over 30 years without offering any financial reward, and have exchanged over 430K emails in the process.<sup>[17]</sup> Similar institutions exist outside the US.<sup>[18]</sup>

### *Vulnerability Markets*

Multiple sales channels exist for researchers seeking monetary compensation. Bug bounty programs, in which researchers are rewarded for reporting directly to the vendor,<sup>[19]</sup> sit at the legitimate end of the spectrum. Black markets, in which criminals offer financial rewards for exploits, sit at the illicit end of the spectrum.<sup>[20,21,14]</sup> Exploit brokers can be considered gray markets existing somewhere between bug bounties and black markets, with legitimacy varying based on who the broker sells to.

These institutions display many properties of traditional markets. For example, bug bounties display upwards sloping supply curves.<sup>[22,13]</sup> Perhaps more surprisingly, black markets have developed enforcement mechanisms that prevent dishonest practices<sup>[14]</sup> and freelancers have declined from 80% to 20% of total participants (as of 2014) as criminal organizations form.<sup>[20]</sup> In terms of outcomes, empirical works show that bug-bounty programs are effective<sup>[23,24]</sup> and efficient<sup>[25,26]</sup> security interventions. We also see that exploits procured in black markets are used by threat actors.<sup>[27]</sup>

Although different sales channels exist, the viability and rewards of each channel will vary depending on the particular exploit. On the supply side, Luna et al.,<sup>[24]</sup> find that experienced researchers display different work patterns to entry-level researchers. In terms of equilibrium price, exploit kits are priced in thousands of dollars,<sup>[20]</sup> and the average bug bounty on the HackerOne platform was just \$318,<sup>[26]</sup> whereas zero-day exploits can be priced in the millions.<sup>[11]</sup> This motivates considering markets for zero-days separately.

### *Zero-Day Markets*

Zero-day exploits take advantage of a security vulnerability that is not known to the software vendor or the wider security community. Such exploits are powerful because two important tools are not available to defenders, namely applying software patches designed to fix the underlying vulnerability and scanning for “signatures,” the behavioral patterns and code of past exploits. This means zero-day exploits can target more devices and be detected less easily than N-day exploits, where N is the number of days since the exploit or vulnerability was public. This section does not exhaustively examine the technical or policy aspects of zero-days but does try to do so for empirical studies of market structure. In terms of technical analysis, Stone<sup>[28]</sup> analyzed the 24 zero-days detected in the wild in 2020, nine of which were variants on “previously disclosed vulnerabilities” or incompletely patched. This raises the question of how markets deal with zero-day variants. Turning to policy, Fidler<sup>[11]</sup> outlines the national and international policy apparatus surrounding zero-days considering issues like export bans that likely impact market participants and structure.

The nature and ethics of zero-day markets were probed at a 2013 workshop,<sup>[29]</sup> which documented how zero-day markets operated largely in the shadows. A year later, Ablon et al.<sup>[20]</sup> assembled a “sparse and inconsistent” table of prices for zero-days and note that whether prices are increasing or decreasing is an open question. Table 2 of Meakins’ work<sup>[30]</sup> provided a snapshot of pricing for a limited number of vulnerabilities across four different brokers. Interestingly, they show the high-end prices at Western brokers are an order of magnitude higher than at the broker operating in Russia. Table 2 does not differentiate between the properties of an exploit, such as whether physical access or user interaction is required.<sup>[30]</sup>

While the previous papers<sup>[20,30]</sup> opted for a comparative study of multiple brokers, we provide an in-depth study of just one broker. This allows us to identify the longitudinal development of prices and answer the open question of whether prices are increasing.<sup>[20,26]</sup> Although we have only studied the maximum prices quoted by one broker, which is an imperfect proxy of the actual fee paid to researchers. Further, we also collect information about not only the systems targeted in an exploit (as in <sup>[20,30]</sup>), but the capabilities required to use that exploit. The next section describes the process by which exploits are sold, as this sheds light on some of the open questions.

## RESEARCHER-BROKER RELATIONS

The supply side of zero-day markets consist of a researcher selling an exploit to the broker. We describe the process using a mixture of testimonies from researchers,<sup>[31,32]</sup> the websites of brokers<sup>[15,33]</sup> and research articles<sup>[29,34]</sup>. The seller contacts the broker, whether through connections or directly, and shares the exploit's specifications. Important criteria are:

- ◆ The targeted software, OS and architecture.
- ◆ The type of vulnerability (e.g., use-after-free).
- ◆ Attack vector (website, document, etc).
- ◆ Reliability (typically probability of success needs to be > 90%).
- ◆ Speed of exploitation (on the order of seconds).
- ◆ Does the exploit crash running processes?
- ◆ Is user interaction required?
- ◆ Does the exploit work with default settings?
- ◆ Any other relevant limitations.

The broker responds with a non-binding preliminary offer, usually less than the publicly advertised maximum payout, after taking limitations into account. The seller may then submit their exploit for evaluation by the broker. It is customary to allow for an assessment period of up to two weeks.<sup>[31,15]</sup> In this time the broker tests the zero-day and compares their result to the specifications provided by the seller. Given no contract has been signed before verification, the seller generally has to trust the broker not to share the information about the exploit,<sup>[35]</sup> although some brokers sign a contract with the seller before the submission.<sup>[31,33]</sup>

Whether the contract is signed before or after the validation period, the contract specifies: payment terms (warranty), intellectual property rights, exclusivity and support requirements.<sup>[31,32]</sup> The payment is usually spread out over the course of a few months to a year. The contract is contingent on no patch being developed that purposely (or accidentally) fixes the vulnerability underlying the exploit. Depending on the terms of the contract, the seller may be required to either to provide a replacement exploit or forfeit all outstanding payments. This also serves as an incentive to honor possible exclusivity agreements. Previous research indicates that exploits are quite likely to survive this period<sup>[34]</sup> providing they are used responsibly.<sup>[31]</sup> This contractual structure is sometimes referred to as “split the risk.”

Compromising exclusivity, coined “double dipping” by Schwartz,<sup>[31]</sup> by selling the same exploit to multiple parties is risky due to the small size of the market. With estimates of active researchers ranging from 400<sup>[31]</sup> to 1500<sup>[35]</sup> and a much smaller number of brokers and buyers, the discovery of dishonesty becomes quite likely. The seller would thus incur legal troubles and reputational loss.<sup>[31]</sup>

Until 2015, brokers did not publicly advertise prices.<sup>[29]</sup> Instead, market participants needed to navigate informal professional networks, a sign of an immature market. Since then, at least two brokers have begun to publicly advertise prices paid to researchers (notably omitting what buyers pay).<sup>[35,33]</sup> Our research studies one of these brokers.

**RESEARCH DESIGN**

Our goal is to capture the development of exploit prices offered by Zerodium. This broker buys zero-day exploits from freelance developers and provides them to government agencies.<sup>[15]</sup> Their website lists prices for different exploits, in a graphic designed to resemble a periodic table, an example of which is depicted in Figure 1. It should be noted that the prices listed are the maximal amount, and actual payouts depend on “quality of the submitted exploit (full or partial chain, supported versions/systems/architectures, reliability, bypassed exploit mitigations, default vs. non-default components, process continuation, etc.).”<sup>[15]</sup>

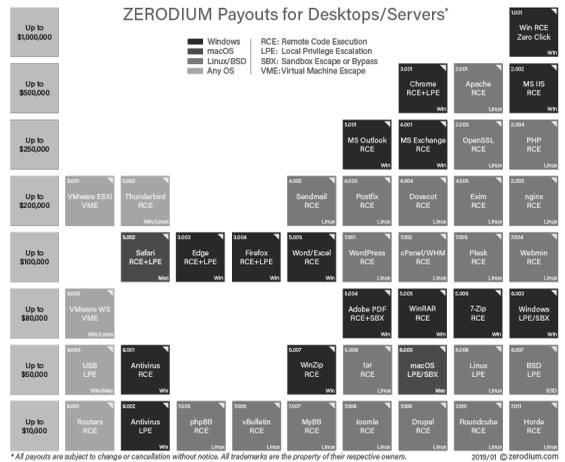


Figure 1: The Figure lists different tiers of prices on the left-most column and a brief description of an exploit in each square, for example “Chrome RCE+LPE on Windows OS” and a price on the left-hand side is bought for “up to \$500,000.”

**Data Collection**

We collected the longitudinal data via the Internet Archive's Wayback Machine<sup>[36]</sup>. Using their CDX API, we determined that the price table has changed only seven times since the program's inception in 2015. The Internet Archive samples are published much more frequently (243 times since 2015) than new prices, which increases confidence that our sample does not miss data.

The tables are available only as images, which we transcribed manually. We extracted each tile from the seven price tables. We then combined exploits that have the same name but are listed in different tables (i.e., at different times) to see how prices vary over time. Thus, we recover a sample of 205 unique types of exploits. This leads to a sparse and irregular panel data set from 2015 until the present, in which the quoted price is the dependent variable.

We further classify the exploits in order to run linear regressions, we chose this functional form for interpretability.<sup>1</sup> For each advertised price, we calculate the number of days since our first observation.

1 Future work will explore models tailored to our irregular, auto-correlated panel data that contains outliers.

Statistic	N	Mean	St. Dev.	Min	Max
price (\$)	543	183.8k	293,063.8	5k	2.5m
days (since start of sample period)	543	846.4	439.3	0	1,387
osandroid	543	0.14	0.3	0	1
osbsd	543	0.01	0.43	0	1
osios	543	0.2	0.4	0	1
oslinux	543	0.2	0.4	0	1
osmac	543	0.04	0.2	0	1
osunspecified	543	0.2	0.4	0	1
oswindows	543	0.2	0.4	0	1
oswindows.phone	543	0.01	0.1	0	1
BrowserTrue	543	0.2	0.4	0	1
EmailTrue	543	0.1	0.3	0	1
MessengersTrue	543	0.1	0.3	0	1
Web.ServerTrue	543	0.1	0.3	0	1
antivirusTrue	543	0.02	0.1	0	1
Requires.Local.AccessTrue	543	0.05	0.2	0	1
Local.Privilege.EscalationTrue	543	0.3	0.5	0	1
Mitigation.BypassTrue	543	0.01	0.1	0	1
Remote.Code.ExecutionTrue	543	0.7	0.5	0	1
Full.Chain.with.PersistenceTrue	543	0.03	0.2	0	1

Table 1: Descriptive data. All rows apart from price and days are dummy variables. The mean value column describes the proportion of the 543 vulnerabilities for which that property is true. For example, 14% of the exploits target Android devices and 70% provide remote code execution functionality.

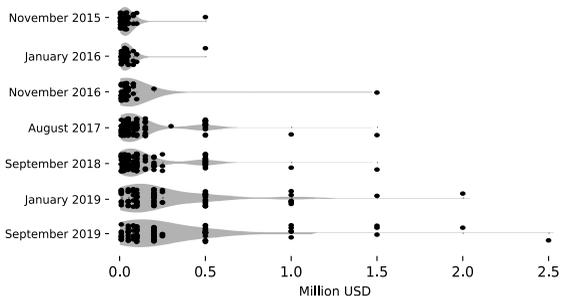


Figure 2: Univariate scatter plot of exploit bounties offered at the different captured snapshots. One dot represents one exploit. Violin plots are added to visualize the concentration of exploit types around certain price bands.

Model 1 shows that around 20% of the variance can be explained by temporal fixed effects. Models 2-4 isolate the explanatory power of the dummy variables based on targeted OS, targeted application, and exploit type respectively. The targeted OS has the least explanatory power (Model 2), likely because each OS contains a range of applications with varying levels of interest and security. For example, an exploit of WhatsApp messenger has the same price for both the iOS or Android version. The targeted application (Model 3) and type of exploit (Model 4)

2 A dummy variable is equal to 1 if the property is true, and 0 otherwise. For example, the dummy variable BrowserTrue is equal to 1 if the exploit targets a browser application and 0 otherwise.

3 We used the OS labels from the price table, using unspecified when none was provided, which was a minority of cases. To create the other categories (vendor, product type and exploit type) we automatically searched the exploit names for certain keywords. For instance, an exploit whose name contained any of the keywords "messenger," "signal," "telegram," "whatsapp" or so on was categorized under "Messenger." We chose these categories with the intent of grouping similar exploits, to allow for descriptive modelling.

We then build several dummy variables.<sup>2</sup> We extracted<sup>3</sup> explanatory variables like the vendor and type of product (e.g., messenger, browser, etc.), as well as the kind of exploit (remote code execution, local privilege escalation, etc.). These can be seen in Table 1.

## RESULTS

Figure 2 shows how exploit prices are distributed. The majority of prices are \$100k or less, especially in the early years of our sample. The most expensive exploits inflate in price rapidly from 2016, growing by 500%. Prices cluster around salient values, such as the cluster at \$500K that emerged from 2017 onward. Negotiated prices may not display such clustering.

We then ran a number of regressions to understand what explains this variance. Table 2 contains a number of log-linear models (1 through 7, with column heads at the top of the table) with the exploit's dollar price as the dependent variable. We opted for log-linear over linear models after inspecting QQ plots, but for comparison we include the equivalent linear regressions in Table 3 in the appendix.

EXPLOIT BROKERS AND OFFENSIVE CYBER OPERATIONS

Model	1	2	3	4	5	6	7
android		1.740***			0.828***		0.493**
		-0.257			-0.229		-0.167
bsd		0.502			0.095		-0.233
		-0.649			-0.52		-0.502
ios		2.063***			0.991***		0.657***
		-0.256			-0.232		-0.169
linux		0.655*			0.388		0.107
		-0.259			-0.212		-0.155
mac		0.674*			0.147		-0.15
		-0.316			-0.271		-0.234
windows		1.188***			0.783***		0.499**
		-0.255			-0.21		-0.156
windows phone		1.444*			-0.768		-0.937
		-0.61			-0.518		-0.521
BrowserTrue			0.249*		0.266*		0.236*
			-0.12		-0.106		-0.108
EmailTrue			0.036		0.124		0.125
			-0.14		-0.126		-0.128
MessengersTrue			1.821***		1.180***		1.161***
			-0.137		-0.14		-0.142
Web.ServerTrue			-0.876***		-0.593***		-0.589***
			-0.136		-0.131		-0.134
antivirusTrue			-0.947**		-1.019***		-1.055***
			-0.297		-0.252		-0.255
Requires.Local.AccessTrue		-0.495*	-0.377*		-0.358*		
				-0.197	-0.167		-0.17
Local.Privilege.EscalationTrue		1.054***	0.482***		0.542***		
				-0.091	-0.095		-0.095
Mitigation.BypassTrue		1.183*	1.074*		1.077*		
				-0.563	-0.466		-0.474
Remote.Code.ExecutionTrue		0.633***	0.591**		0.587***		
				-0.097	-0.096		-0.097
Full.Chain.with.PersistenceTrue		3.164***	2.758***		2.930***		
				-0.25	-0.241		-0.234
days						0.001***	0.001***
						-0.0001	-0.0001
Constant	10.167***	9.931***	10.296***	9.275***	9.384***	10.191***	9.381***
	-0.191	-0.174	-0.164	-0.178	-0.159	-0.111	-0.123
Observations	543	543	543	543	543	543	543
R2	0.203	0.388	0.473	0.487	0.662	0.186	0.647
Adjusted R2	0.194	0.373	0.462	0.477	0.647	0.185	0.635

Note: \*p<0.05; \*\*p<0.01; \*\*\*p<0.001

Table 2: Linear regressions with log-transformed price (\$) as the dependent variable. Time-based fixed effects included for all but Model 6 and 7.

effect size, which is particularly striking given Figure 6 shows the broker did not trade such exploits when it was launched in 2015. Exploits of web servers (*Web.ServerTrue*) and anti-virus products (*antivirusTrue*) are comparably cheaper, as seen in Figure 6.

Turning to properties of the exploit, we find a number of reassuringly obvious results. The variable for full-chain-persistence has the largest effect size, which is unsurprising given such an exploit can be used to compromise any other application on the device. Conversely, the least powerful exploits – those that require local access (e.g., to insert a USB driver) – are comparably cheaper, which can be seen in the regression coefficient *Requires.Local.AccessTrue*. Figure 7 shows the average price for each type of exploit over time.

have more explanatory power, with individual dummies contributing a lot—removing the messenger and full-chain-persistence dummies lead to 38% and 33% reductions in  $R^2$  in Model 3 and Model 4 respectively.

Comparing the  $R^2$  of Model 5 and Models 2-4 shows that the variables have additional predictive power when taken together, and so we proceed by analyzing this model. The coefficients for targeted OS in Model 5 suggest that exploits targeting mobile devices (e.g., Android and iOS) are more expensive than those targeting desktops, which can also be seen in Figures 4 and 5. Figure 3 shows the total bounties available has been consistently high for Apple, but Google has recently overtaken Microsoft, likely due to the increasing cost and availability of exploits targeting mobile devices.

Turning to specific products, Model 5 shows that *MessengerTrue* (e.g., WhatsApp, iMessage, Signal and so on) has the second largest

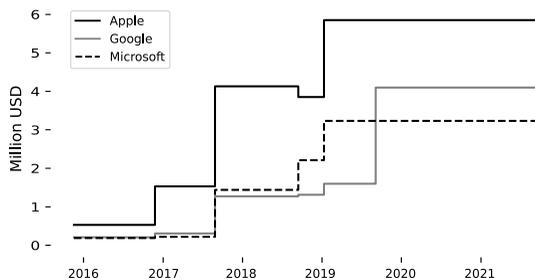


Figure 3: The sum of all exploit bounties for certain vendors, from 2015 until present.

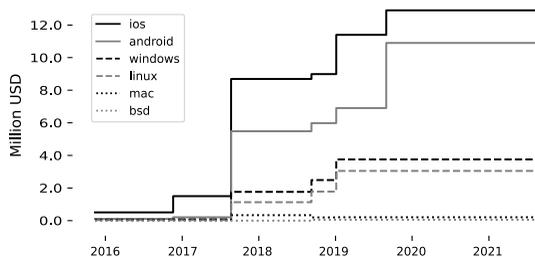


Figure 4: The sum of all exploit bounties by OS, from 2015 until present.

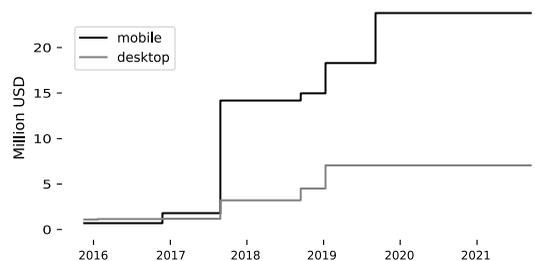


Figure 5: A comparison of total bounties offered for mobile versus desktop/server systems (2015 until present).

justified by the broker receiving multiple exploit submissions.<sup>[38]</sup> This suggests that bursts in the supply of exploits can drive down prices, although we doubt buyers see an equivalent reduction in price. We cannot observe whether price fluctuations influence researcher attention. Ultimately, we can only caution against reading too much into prices and call for a more sophisticated economic analysis in future work.

We can, however, make a number of reliable observations. The monetary cost of exploiting certain systems is a consideration in itself. For example, exploits of modern messenger applications can now cost over a million dollars. These costs no doubt drive law enforcement's calls for "exceptional access,"<sup>[39]</sup> whereby technology companies would be required to build-in backdoor vulnerabilities that governments can access in response to an incident and/or investigation.

High exploit prices feed into the challenge of retaining security researchers, who can leave and sell their expertise to the highest bidder, this impacts both government agencies and the

All the longitudinal figures show that exploits generally become more expensive over time. This can also be observed in the days variable in Model 7 – here we impose a linear relationship between the number of days since the first set of prices and that exploit's price. The linear model in the generally appendix (Table 3) shows a mean increase of \$234 per day in our observation period, which translates into 44% growth per annum. Also inspecting the fixed effects on each time period, we find larger effects for the later periods.

## DISCUSSION

We first consider what these results tell us about wider debates, and then reflect on using exploit brokers as a data source.

### *Interpreting prices*

Interpreting prices is notoriously difficult.<sup>[37]</sup> Are prices high because many governments target that system (demand driven) or because that product is particularly secure (supply driven)? In 2020, the broker announced that purchases of iOS exploits were temporarily suspended, which was

vendors of these products.<sup>[10]</sup> These problems will persist given that the average price of an exploit increases by \$234 per day (see Table 3) or 44% per year. This speaks to the open question of whether exploit prices are increasing.<sup>[20]</sup>

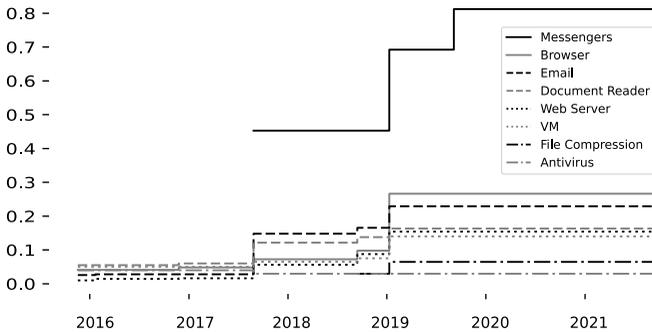


Figure 6: Comparing the average prices of exploits for different product categories, from 2015 until present.

### Omissions

We observed a lack of exploits that could conceivably cause physical damage targeting Industrial Control Systems or even IoT devices. This is likely because ICS systems display a different security model from mobile applications, not to mention the increased barriers to conducting ICS research. The majority (64%) of ICS vulnerability advisories had no patch, and instead relied on network segmentation to avoid compromise.<sup>[40]</sup> Thus, only exploits that provide “access to a control system network”<sup>[40]</sup> are valuable. Similarly, IoT devices are often insecure by default.<sup>[41]</sup> Exploit markets are unlikely to exist where the barrier to compromise is low enough for internal expertise.

An alternative explanation for this omission is that other brokers or criminal groups trade in exploits providing such access, or even that this broker trades in them without announcing prices. More generally, that Zerodium<sup>[15]</sup> and Crowd-Fense<sup>[33]</sup> offer public prices suggests that trading in these specific exploits is not deemed to incur prohibitive reputation or legal risk. We return to the question of cyber norms in the final section.

### Data Sources

Building an empirical picture of offensive cyber operations runs against the interests of those conducting such operations. While circumstances can exist under which belligerents claim credit for cyber operations,<sup>[42]</sup> secrecy is the default.<sup>[43]</sup> The dynamics of offensive cyber will outpace time-lagged sources used by traditional intelligence studies like declassified documents<sup>[44,45]</sup> or officers retiring and then revealing details.<sup>[46]</sup> To address this, cyber strategy scholars have turned to novel data sources.

The ease of duplicating operational computer code leads to publications by third parties like governments,<sup>[47]</sup> private firms,<sup>[48]</sup> and academics.<sup>[49,50]</sup> Each samples in a different way, leading to very different pictures of cyber operations. Egloff<sup>[47]</sup> argues that beyond establishing facts (sense-making), state-led attributions also aim to influence public and elite opinion—this sampling bias would lead one to believe cyber operations are primarily conducted by a handful of governments against the West.<sup>[51,Table V]</sup> In contrast, the Citizen Lab's analyses of malware campaigns<sup>[49,50]</sup> suggest journalists are the primary target. Stretching the definition of offensive

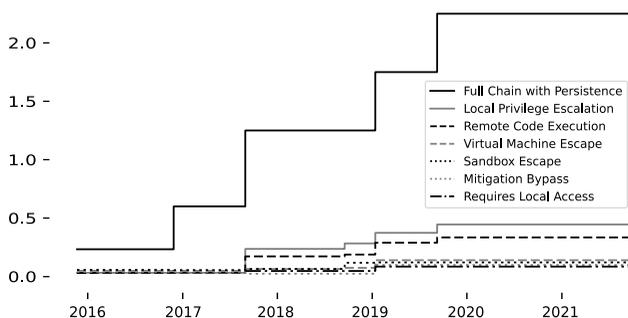


Figure 7: Comparing the average prices of different kinds of exploits, from 2015 until present.

cyber to include information operations, empirical sources like Twitter<sup>[52,53]</sup> and message boards<sup>[54]</sup> suggest the public is the primary target. Thus, the choice of evidence base leads to a different characterization of offensive cyber operations.

We argue that our data supplements existing data sources. In particular, relying on analyses of operational code leads to a reporting bias in that it necessarily ignores undetected operations. An additional strength of our data is that markets are updated in real time, whereas code analysis takes time and declassification takes even longer.

*Limitations*

Our findings are based on maximum payouts, whereas real payouts are negotiated and likely much lower. Thus, our data over-inflates the demand and supply of exploits. Zerodium’s publishing of disclosures likely serves the commercial interest of generating publicity, and so Zerodium’s prices may fundamentally differ from those of other brokers. For example, Meakins<sup>[30]</sup> showed that brokers who operate in Russia quote far lower prices. Beyond limitations in the data, our modelling was crude and requires further refinement.

## FUTURE OF OFFENSIVE CYBER

Exploit prices quoted by brokers provides insights into offensive cyber operations. We discovered that:

- 1) Exploits of iOS and windows are the most expensive for mobile and desktop respectively with mobile exploits higher on average.
- 2) Exploits of messengers and browsers are more expensive than those of web servers and anti-viruses.
- 3) Exploits requiring local access are comparably inexpensive.

We also observed a general trend towards exploits becoming more expensive over time. So, what does this mean for the future of offensive cyber operations? The rest of this section speculates on three aspects of this question.

### *Could offensive cyber operations be constrained by exploit markets?*

Continued exploit price inflation represents an increasing economic constraint on offensive cyber operations. Scholars of security economics have long argued that increasing the cost to attackers is viable route forward given that perfect security is not achievable.<sup>[55,56]</sup> The resulting

barrier to entry provides a hard ex-ante limit on offensive cyber operations, whereas cyber deterrence imposes ex-post disincentives that rely on victims detecting, attributing, and authorizing a response to offensive cyber operations, each of which is uncertain.

Such constraints vary according to the targeted system and the capabilities of the offensive actor as our regressions show. The future implications are unclear, but it is clear that no-click, remote access exploits are inflating fastest (see Figure 7). As a result, exploits requiring local access are relative bargains. One could speculate that cyber operations targeting domestic actors are becoming relatively more cost-effective because capabilities like physical access to the targeted device are more realistic for domestic actors. Note this also assumes offensive actors are rational, which may not always be the case.

### ***Could offensive cyber operations be constrained by vulnerability researchers?***

First, exploit brokers offer incentives for individuals to leave government agencies, although admittedly higher private-sector salaries are nothing new. These incentives are relatively higher for more talented researchers thus creating staffing problems. This could motivate export controls and other legal limitations on the sale of zero-days.<sup>[11]</sup> Perhaps more interestingly, researchers are paid based on how long the zero-day remains un-patched (see Section 3). Could researchers exert pressure against wanton use of the exploit that increases the likelihood of detection and hence a patch that disrupts the payment plan? This turns on how much market power researchers have.

The number of independent active sellers (between 400<sup>[31]</sup> and 1500<sup>[35]</sup> individuals) relative to buyers (a small number of states conducting OCO) suggest the power is limited. Further, looking at Zerodium's total payouts, \$50 million for exploits since their founding in 2015,<sup>[35]</sup> suggests an annual pay of \$5.5k - 20.8k per researcher. Such estimates should be interpreted in light of researchers having multiple income streams (e.g., multiple brokers, bug bounties, and other security work) and the reality that superstar effects mean a minority collect the majority of payments.<sup>[13]</sup>

### ***How do exploit markets interact with cyber norms?***

Another cost incurred by offensive operations is reputation damage, such as that mediated by norms of responsible state behavior.<sup>[6]</sup> Norms constrain what can be publicly advertised as brokers seek to avoid scandal. Market actors selling offensive cyber appear to have created outrage among journalists who focus on their use by repressive regimes.<sup>[10,57]</sup> Broker's demonstrate their understanding of such reputation risk by establishing “due diligence and vetting process”<sup>[15]</sup>, although we have no further details on what exactly this entails.

Alternatively, one could imagine how brokers quoting a price for a given exploit could legitimize using such exploits, acting as private norm entrepreneurs in doing so.<sup>[7,58]</sup> It could be that these brokers are normalizing the use of exploits for espionage, given that exploits specifically targeting communications (e.g., messaging and email) are among the most common and also have a higher average price. Looking forward, this motivates ongoing analysis of brokers' offerings to understand which systems it is “normal” to target with offensive cyber operation.♥

**ACKNOWLEDGEMENTS**

We would like to thank Rainer Bohme, Max Smeets, Simon Rock, Andrew Dwyer and Amy Ertan for their insightful comments and useful feedback. We are also grateful to the other participants for the fruitful discussion during the author workshop. This research was funded by the Air Force Office of Scientific Research.

**APPENDIX**

Price (\$)	1	2	3	4	5
period					234 <sup>***</sup>
					-25
android	249,135 <sup>***</sup>			-143,682 <sup>***</sup>	-97,025 <sup>***</sup>
	-63,895			-49,100	-35,647
bsd	-6,651			-279,139 <sup>**</sup>	-232,700 <sup>**</sup>
	-161,136			-111,202	-106,807
ios	351,662 <sup>***</sup>			-103,540 <sup>**</sup>	-54,922
	-63,657			-49,655	-35,924
linux	62,229			-191,314 <sup>***</sup>	-142,278 <sup>***</sup>
	-64,342			-45,433	-32,991
mac	40,448			-192,090 <sup>***</sup>	-149,388 <sup>**</sup>
	-78,372			-58,031	-49,898
windows	110,775 <sup>*</sup>			-122,970 <sup>***</sup>	-77,292 <sup>**</sup>
	-63,218			-45,033	-33,211
windows phone	67,613			-999,072 <sup>***</sup>	-981,444 <sup>***</sup>
	-151,481			-110,890	-111,026
BrowserTrue		-12,468		17,671	18,295
		-30,267		-22,740	-22,907
EmailTrue		2,950		52,266 <sup>*</sup>	53,673 <sup>*</sup>
		-35,382		-27,060	-27,361
MessengersTrue		426,659 <sup>***</sup>		365,398 <sup>***</sup>	364,179 <sup>***</sup>
		-34,564		-29,869	-30,189
Web.ServerTrue		-60,188 <sup>*</sup>		19,193	20,056
		-34,370		-28,114	-28,429
antivirusTrue		-112,511		-113,953 <sup>**</sup>	-110,883 <sup>**</sup>
		-74,923		-53,849	-54,361
Local.Privilege.EscalationTrue		192,633 <sup>***</sup>	92,681 <sup>**</sup>	96,774 <sup>***</sup>	
			-20,138	-20,328	-20,257
Mitigation.BypassTrue		197,569	94,563	97,809	
			-124,779	-99,817	-100,937
Remote.Code.ExecutionTrue		139,874 <sup>***</sup>	60,792 <sup>***</sup>	65,631 <sup>***</sup>	
			-21,465	-20,594	-20,737
Requires.Local.AccessTrue		-112,396 <sup>**</sup>	-76,307 <sup>**</sup>	-68,726 <sup>*</sup>	
			-43,641	-35,798	-36,147
Full.Chain.with.PersistenceTrue		1,015,542 <sup>***</sup>	1,153,635 <sup>***</sup>	1,139,252 <sup>***</sup>	
			-55,464	-51,477	-49,843
Constant	21,510	63,916	-168,446 <sup>***</sup>	65,440 <sup>*</sup>	-91,838 <sup>***</sup>
	-43,185	-41,380	-39,452	-33,971	-26,148
Observations	543	543	543	543	543
R2	0.241	0.325	0.494	0.689	0.679
Adjusted R2	0.223	0.311	0.483	0.675	0.668

Note: <sup>\*</sup>p<0.1; <sup>\*\*</sup>p<0.05; <sup>\*\*\*</sup>p<0.01

Table 3: Equivalent linear regressions with log-transformed price (\$) as the dependent variable.

## NOTES

1. Florian J. Egloff and James Shires. The better angels of our digital nature? offensive cyber capabilities and state violence, *European Journal of International Security*, 1-20, 2021.
2. Jacqueline Eggenschwiler and Jantje Silomon, Challenges and opportunities in cyber weapon norm construction *Computer Fraud & Security*, 2018(12):11{18, 2018.
3. Andrew Dwyer, The NHS cyber-attack: A look at the complex environmental conditions of WannaCry, *RAD Magazine*, 44, 2018.
4. John Arquilla and David Ronfeldt, Cyberwar is coming! *Comparative Strategy*, 12(2):141-165, 1993.
5. Thomas Rid, Cyber war will not take place, *Journal of Strategic Studies*, 35(1):5-32, 2012.
6. Martha Finnemore and Duncan B Hollis, Constructing norms for global cybersecurity. *American Journal of International Law*, 110(3):425-479, 2016.
7. Louise Marie Hurel and Luisa Cruz Lobato, Unpacking cyber norms: private companies as norm entrepreneurs, *Journal of Cyber Policy*, 3(1):61-76, 2018.
8. Myriam Dunn Cavely, Cyber-security and private actors. In *Routledge handbook of private security studies*, 89-99. Routledge, 2015.
9. Jamie Collier, Cyber security assemblages: a framework for understanding the dynamic and contested nature of security provision, *Politics and Governance*, 6(2):13-21, 2018.
10. Nicole Perlrot, *This Is How They Tell Me the World Ends: The Cyber-weapons Arms Race*, chapter 10, Bloomsbury Publishing, 2021.
11. Maylin Fidler, Anarchy or regulation: Controlling the global trade in zeroday vulnerabilities, *PhD diss.*, Freeman Spogli Institute for International Studies, Stanford University, 2014.
12. Ross Anderson and Tyler Moore, The economics of information security, *science*, 314(5799):610-613, 2006.
13. Kiran Sridhar and Ming Ng, Hacking for good: Leveraging hacker one data to develop an economic model of bug bounties, *Journal of Cybersecurity*, 7(1):tyab 007, 2021.
14. Luca Allodi, Marco Corradin, and Fabio Massacci, Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketers learned, *IEEE Transactions on Emerging Topics in Computing*, 4(1):35-46, 2015.
15. Zerodium, Frequently Asked Questions, [www.zerodium.com/faq.html](http://www.zerodium.com/faq.html), 2021.
16. Charlie Miller, The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales, In *Workshop on the Economics of Information Security*, 2007.
17. Kiran Sridhar, Allen Householder, Jonathan M. Spring, and Daniel W. Woods, Cybersecurity information sharing: Analysing an email corpus of coordinated vulnerability disclosure, In *Workshop on the Economics of Information Security*, 2021.
18. Leonie Maria Tanczer, Irina Brass, and Madeline Carr, CSIRTs and global cybersecurity: How technical experts support science diplomacy, *Global Policy*, 9:60-66, 2018.
19. Rainer Bohme, A comparison of market approaches to software vulnerability disclosure, *International Conference on Emerging Trends in Information and Communication Security*, 298-311, Springer, 2006.
20. Lillian Ablon, Martin C Libicki, and Andrea A Golay, *Markets for cyber-crime tools and stolen data: Hackers' bazaar*, RAND Corporation, 2014.
21. Luca Allodi and Fabio Massacci, Comparing vulnerability severity and exploits using case-control studies, *ACM Transactions on Information and System Security (TISSEC)*, 17(1):1, 2014.
22. Mingyi Zhao, Jens Grossklags, and Peng Liu, An empirical study of web vulnerability discovery ecosystems, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1105-1117, ACM, 2015.
23. Sam Ransbotham, Sabyaschi Mitra, and Jon Ramsey, Are markets for vulnerabilities effective? *MIS Quarterly*, 43-64, 2012.
24. Donatello Luna, Luca Allodi, and Marco Cremonini, Productivity and patterns of activity in bug bounty programs: Analysis of hackerone and google vulnerability research, *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 67, ACM, 2019.
25. Matthew Finifter, Devdatta Akhawe, and David Wagner, An empirical study of vulnerability rewards programs, *USENIX Security Symposium*, 2732-88, 2013.
26. Thomas Walshe and Andrew Simpson, An empirical study of bug bounty programs, *2020 IEEE 2nd International*.

## NOTES

27. Chris Grier, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, et al. Manufacturing compromise: the emergence of exploit-as-a-service, *Proceedings of the 2012 ACM conference on Computer and communications security*, 821-832, ACM, 2012.
28. Maddie Stone, The state of 0-day in-the-wild exploitation, USENIX Association, February 2021.
29. Serge Egelman, Cormac Herley, and Paul C. van Oorschot. Markets for zero-day exploits: Ethics and implications, *Proceedings of the 2013 New Security Paradigms Workshop*, NSPW '13, 41-46, New York, 2013, Association for Computing Machinery.
30. Joss Meakins, A zero-sum game: the zero-day market in 2018, *Journal of Cyber Policy*, 4(1):60-71, 2019.
31. Maor Shwartz, Selling 0-days to governments and offensive security companies, Blackhat, 2019.
32. Vlad Tsyrlkevich, Hacking team: a zero-day market case study, [www.tsyrlkevich.net](http://www.tsyrlkevich.net), 2015.
33. Crowdfense, Bug Bounty Program, [www.crowdfense.com/bug-bounty-program.html](http://www.crowdfense.com/bug-bounty-program.html), 2021.
34. Lillian Ablon and Andy Bogart, Zero Days, Thousands of Nights, RAND Corporation, Santa Monica, CA, 2017.
35. Zerodium, [www.zerodium.com](http://www.zerodium.com), 2022.
36. The Internet Archive, *The Wayback Machine*, [www.web.archive.org](http://www.web.archive.org), 2021.
37. Scott Sumner, Never reason from a price change, [www.themoneyillusion.com/never-reason-from-a-price-change/](http://www.themoneyillusion.com/never-reason-from-a-price-change/), 2010.
38. @Zerodium. We will NOT be acquiring any new Apple iOS LPE, Safari RCE, or sandbox escapes for the next 2 to 3 months due to a high number of submissions related to these vectors. Prices for iOS one-click chains (e.g. via Safari) without persistence will likely drop in the near future. [twitter.com/Zerodium/status/1260541578747064326](https://twitter.com/Zerodium/status/1260541578747064326), May 2020.
39. Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G Neumann, et al. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1):69-79, 2015.
40. Dragos, Inc. ICS cybersecurity year in review 2020, 2021.
41. Irina Brass, Leonie Tanczer, Madeline Carr, and Jason Blackstock. Regulating iot: enabling or disabling the capacity of the internet of things? *Risk&Regulation*, 33:12-15, 2017.
42. Michael Poznansky and Evan Perkoski. Rethinking secrecy in cyberspace: The politics of voluntary attribution. *Journal of Global Security Studies*, 3(4):402-416, 2018.
43. Dakota S Rudesill. Cyber operations, legal secrecy, and civil-military relations. In *Reconsidering American Civil-Military Relations*, pages 245-262. Oxford University Press, 2020.
44. Len Scott and Peter Jackson. The study of intelligence in theory and practice. *Intelligence & National Security*, 19(2):139-169, 2004.
45. Richard Aldrich. 'grow your own': cold war intelligence and history supermarkets. *Intelligence and National Security*, 17(1):135-152, 2002.
46. Nigel West. Fiction, faction and intelligence. *Intelligence & National Security*, 19(2):275-289, 2004.
47. Florian J Egloff. Public attribution of cyber intrusions. *Journal of Cybersecurity*, 6(1):tyaa012, 2020.
48. Juan Andrés Guerrero-Saade. The ethics and perils of apt research: an unexpected transition into intelligence brokerage. In *Proceedings of the 25<sup>th</sup> Virus Bulletin International Conference*, 2015.
49. Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. Missing link: Tibetan groups targeted with 1-click mobile exploits. Citizen Lab Research Report No. 123, 2019.
50. Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. The great ipwn: Journalists hacked with suspected nso group imessage 'zero-click' exploit. Citizen Lab Research Report No. 135, 2020.
51. Brandon Valeriano and Ryan C Maness. The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, 51(3):347-360, 2014.
52. Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. Disinformation warfare: Understanding state-sponsored trolls on twitter and their influence on the web. In *Proceedings of the 2019 World Wide Web Conference*, 218-226, 2019.
53. Darren L Linvill and Patrick L Warren. Troll factories: Manufacturing specialized disinformation on twitter. *Political Communication*, 37(4):447-467, 2020.

**NOTES**

54. Savvas Zannettou, Tristan Caulfield, William Setzer, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. Who let the trolls out? towards understanding state-sponsored trolls. In Proceedings of the 10th ACM Conference on Web Science, 353–362, 2019.
55. Marco Cremonini and Patrizia Martini. Evaluating information security investments from attackers perspective: the return-on-attack (ROA). In Workshop on the Economics of Information Security, 2005.
56. Ross Anderson. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2020.
57. Cory Doctorow. Cyber-mercenaries helped saudis hack an NYT reporter. <https://pluralistic.net/2021/10/24/breaking-the-news/#kingdom>, 2021.
58. Nancy Ayer Fairbank. The state of microsoft?: the role of corporations in international norm creation. *Journal of Cyber Policy*, 4(3):380–403, 2019.





# Democracies and the Future of Offensive (Cyber-Enabled) Information Operations

---

Dr. Bryan Nakayama

## ABSTRACT

*Cyber-enabled information operations that exploit social media to shape narratives and societal perception vex Western democracies which have long treated the free flow of information as a virtue. Despite these tensions, Western democracies have sought to adapt their cyber forces both to counter and to manipulate social media and other information operations as an offensive weapon. This article evaluates how these democracies thus far have responded to information operations with a focus on offensive information and cyber operations. The article analyzes three topics relevant to the future of democracies and cyber-enabled information operations. First, is an explanation as to why Western democracies failed to anticipate the threat of cyber-enabled information operations. Second, the article catalogs and compares how four major Western democracies have responded to information operations—US, UK, France, and Germany. The final section evaluates whether and how democracies should practice offensive cyber-enabled information operations, and why, in the end, the article concludes that democracies should avoid offensive cyber-enabled information operations because they pose three tensions that undermine democracy: Internet fragmentation, violations of democratic norms, and blowback.*



**Bryan Nakayama**, a visiting lecturer of International Relations at Mount Holyoke College, focuses on the intersection of emerging technologies and warfare, with emphasis on cyber and information warfare. He is currently working on a book entitled *“From Aerospace to Cyberspace: The Evolution of Domains of Warfare”* that explains the rise of new domains and ways of warfare. [bnakayam@mtholyoke.edu](mailto:bnakayam@mtholyoke.edu)

## INTRODUCTION

A common belief early in the information age was that the free flow of information in cyberspace reinforced democracy.<sup>[1]</sup> Scholars and policymakers tended to focus on the impacts of authoritarian attempts to restrict and censor—setting up a conflict between democratizing flows of information and authoritarian censorship. By the mid-2010's indications began surfacing that censorship narrowly understood as filtering information was no longer the only threat to the free flow of information as states increasingly turned to armies of online commenters to shape social media narratives. These efforts to shape social media came to the forefront with the revelations that Russia targeted the 2016 US presidential election with information operations leveraging the scale and reach of American social media platforms.<sup>[2]</sup> After the US experienced this “strategic surprise,” emergent campaigns targeting other Western democracies have brought to the fore questions over how democracies should approach modern cyber-enabled information operations.<sup>[3]</sup> At the same time that democracies are enhancing their defenses against information threats, they are also integrating information warfare responsibilities into their cyber military organizations, thereby raising a host of normative concerns over the democratic practice of offensive cyber-enabled information operations.

This article explains how democracies have responded to cyber-enabled information operations and discusses whether they should use offensive cyber-enabled information operations for their own goals. Recognizing ongoing terminological debates around what constitutes a “cyber-enabled information operation,” this article treats them as information operations that leverage means and dynamics unique to cyberspace—with a particular focus on operations targeting social media.<sup>[4]</sup> These information operations threaten democracies insofar as they disrupt information flow and quality,

and limited censorship needed to inform democratic debate, and they undermine social trust and faith in news media.<sup>[5]</sup> While there has been extensive debate and policy focus on how democracies are responding to cyber-enabled information operations, there has been relatively little critical evaluation of whether democracies should conduct offensive information operations.<sup>[6]</sup> This is a necessary debate as democracies update doctrine and expand the role that their cyber forces place in information warfare.

First discussed is why Western democracies failed to effectively anticipate cyber-enabled information operations, followed by an overview of how democracies have responded across two dimensions: domestic policy and foreign policy. Next offensive information operations by democracies, along with the caveat that a full embrace of these operations risks accelerating Internet fragmentation and domestic blowback. The conclusion argues that democracies on-balance should refrain from cyber-enabled information operations and focus on denial strategies against adversaries using them.

### *Why Surprise?*

Reflecting on the relative inattention paid to how non-Western states have characterized contemporary information warfare, U.S. Cyber Command (USCYBERCOM) historian Michael Warner observes that “millions of Americans and Europeans...view their inherently liberal outlook as no more ideological than breathing, as the pragmatic response to the reality of all unbiased minds. In the same manner, they regard the Internet as something apolitical, as a public utility.”<sup>[7]</sup> Another commentator noted that this is because Western democracies generally assume that free flowing information is politically and economically empowering.<sup>[8]</sup> Thus, before the rise of authoritarian cyber-enabled information operations, Internet-accessible information was generally viewed as beneficial, as opposed to being a conduit for political manipulation.

This set of beliefs hinges on the epistemological assumption of the marketplace of ideas – that debate in democratic media environments culls incorrect information and produces a form of consensus truth,<sup>[9]</sup> and the Internet enables flows of information that serves as the grist of democratic debate, thereby strengthening democracy by increasing accountability and allowing for grassroots political organization.<sup>[10]</sup> The Internet also expanded the economic reach of US and Western firms by insofar as developing and accessing new markets. This perspective originated in the 1990’s from the initial set of utopian beliefs in the West that the information age and cyberspace would revolutionize politics by deconcentrating economic and political power.<sup>[11]</sup>

US policymakers believed in these salutary effects and made it a foreign policy goal during the 1990’s and 2000’s to promote the spread of the Internet. One key US program was Democracy Promotion during the late 2000’s in which the State Department trained activists on how to bypass Internet filtering systems in authoritarian states. Secretary of State Clinton characterized censorship and filtering as an attack on the public’s Internet use, making censorship

circumvention a critical element of achieving Internet freedom. Russia and China viewed these programs integral to a larger battle between their political cultures and Western liberalism—the Arab Spring, color revolutions, and domestic protests all Internet driven and dominated by Western values, which drove their approach to the Internet and cyberspace.<sup>[12]</sup> Over the 2010’s Russia and China increasingly turned to large-scale narrative shaping and information disruption on social media as a means of censorship to preserve political stability.<sup>[13]</sup>

Debate over the security consequences of cyberspace often focused on the potential for a devastating surprise offensive cyberspace operation or “Cyber-9/11,” which inspired discussion as to whether cyberspace operations would constitute a potent and independent form of military force akin to kinetic warfare.<sup>[14]</sup> More recently, scholarship has focused more on how cyberspace operations shape state behavior through longer-term cumulative effects or as intelligence activities.<sup>[15]</sup> Thus, debates over cyber threats has tended to focus on the potential consequences of infrastructural degradation instead of the manipulation of perception through information operations.<sup>[16]</sup> As Francois and Lin write: Russian information operations “did not register as a cyber threat according to the accepted conventions of the field, and...did not correspond to a clear and narrow type of threat in traditional cyber conflict literature until after their occurrence and nationwide exposure.”<sup>[17]</sup> The broader social reception of the rise of cyberspace and information technology shaped scholarly and political expectations such that the Russian information operations emerged as a novel threat that challenged existing frameworks by which Western democracies assessed cyberspace threats.

### ***How Western Democracies Have Responded***

Fierce, jingoistic rhetoric of some policymakers notwithstanding, polling and experimental research indicate that the US and UK likely will not support retaliation with force unless cyber or information operations create lethal effects.<sup>[18]</sup> In lieu of using force, scholars have suggested several alternative responses, e.g., domestic regulation of social media,<sup>[19]</sup> policies that revitalize democratic debate and domestic information environments,<sup>[20]</sup> creation of norms against offensive cyber-enabled information operations,<sup>[21]</sup> and creation of a separate democratic intranet.<sup>[22]</sup>

In response to cyber-enabled information operations Western democracies including the US, UK, France, and Germany typically elevate and integrate information operations with existing military cyber organizations, and, other than the proposed democratic intranet, have pursued some combination of the aforementioned domestic proposals. This section briefly surveys early 2022 efforts by these four named democracies to counter and integrate cyber-enabled/information operations through domestic policy, military organization, and doctrine, and closes with observations focused on cyber-enabled information operations in Russia’s 2022 invasion of Ukraine.

### *United States*

As host to many of the world's dominant technology and social media firms such as Google, Microsoft, Twitter, and Facebook, the US is powerfully positioned to control and manage information operations, but the government has yet to meaningfully legislate the governance or structure of such operations. Congress considered the "Honest Ads Act" in 2017, which would increase disclosure and archiving requirements for political advertising on social media, but little legislative progress has occurred in the intervening years.<sup>[23]</sup> Instead, the US has focused on using law enforcement,<sup>[24]</sup> diplomatic,<sup>[25]</sup> sanctions,<sup>[26]</sup> and military measures.

The US pioneered the military approach to cyber-threats with the 2009 creation of USCYBERCOM, yet this focus did not adequately anticipate information operations that leveraged social media.<sup>[27]</sup> Initial cyberspace operations doctrine, such as the Air Force *AFDD 3-12*, explicitly distinguished cyber and information operations stating that they were distinct.<sup>[28]</sup> However, the Russian campaign against the US presidential election pushed the US military to take seriously the relationship between cyber and information operations with recent doctrine explicitly acknowledging this link.<sup>[29]</sup> At the same time that the link between information and cyber operations gained greater acknowledgment in doctrine, USCYBERCOM and the services have been moving to better integrate information operations into their respective cyber units.<sup>[30]</sup> However, the effectiveness of this integration is in question as conceptual slippage between the reality and perception of information operations persists in debates over information operations.<sup>[31]</sup> The US today is nesting its military response to cyber-enabled information operations under the aegis of its broader cyber operations framework.

Reflecting these doctrinal and organizational changes, the US military has responded to adversary information operations by employing both cyber and information operations. First, employing traditional cyberspace operations will deny adversaries the ability to conduct information operations. This can be seen in the 2018 USCYBERCOM operation, which disrupted the Internet Research Agency's internet access, thereby preventing it from accessing social media.<sup>[32]</sup> Second, while fewer details about precise methods are known the US military has countered disinformation campaigns—such as those that have targeted NATO exercises—with counter-narratives.<sup>[33]</sup> Whether these involved bot farms or other large-scale efforts to shape social media is unclear, similarly there have been no reported instances of the military seeking to shape domestic narratives. While the US had an early lead in cyberspace operations, it is rapidly expanding its information operations capability.<sup>[34]</sup>

### *United Kingdom*

The UK's domestic policy response to information operations has intersected with a broader debate over how to manage harmful Internet content. As of 2021, the UK parliament has been debating a sweeping "Online Safety Bill" which would address a range of issues related to online content, of which tackling state-sponsored disinformation is only a part. The bill's emphasis on content moderation has drawn criticism over concerns that it may harm the

capacity for free expression.<sup>[35]</sup> To counter disinformation there also have been national education campaigns to increase societal resilience and otherwise how best to discern disinformation and evaluate news sources.<sup>[36]</sup>

Outside of domestic policy, the UK's military has expanded and integrated information operations capabilities into its military cyber forces. The second edition of the Cyber Primer argues that there is substantial overlap between information operations and cyber operations, but they are distinguished on the basis of the operating environment: cyber operations are conducted in cyberspace whereas information operations are conducted across domains.<sup>[37]</sup> Organizationally, the UK first created the National Security Communications Unit in 2018,<sup>[38]</sup> however, there is little publicly available information about the unit's activities. In 2019, the British Army re-activated and re-organized the 6th (United Kingdom) Division which is a multi-disciplinary unit tasked with integrating cyber, information, and electronic warfare.<sup>[39]</sup> Finally, in 2021 the National Cyber Force was founded, and the 2022 National Cyber Strategy document identified countering online disinformation and defending democratic integrity as key functions of the force.<sup>[40]</sup>

Like the US the UK has countered information threats with cyber and information operations. The UK conducted operations against Daesh—targeting their ability to spread propaganda online.<sup>[41]</sup> Information operations conducted by the UK have supported NATO operations by defending against false or exaggerated narratives.<sup>[42]</sup> One notable area of activity where the UK has combined cyberspace and information operations has been in responding to coronavirus misinformation. While details are thin it was revealed in 2020 that the British Army's 77th Brigade was monitoring and acting against foreign coronavirus misinformation campaigns in conjunction with GCHQ. While no details were reported, one account credited GCHQ with use of cyber operations to take down websites that were spreading misinformation.<sup>[43]</sup>

### *France*

Unlike the UK and US, France has enacted aggressive and controversial domestic policy to counter information operations. In 2018 the French parliament approved an anti-misinformation law that centered on the news environment surrounding elections and empowered a range of actors to punish and restrict the flow of misinformation. The law defines misinformation as "inexact allegations or imputations, or news that falsely report facts, with the aim of changing the sincerity of a vote." Individuals, political parties, and the government are allowed to report misinformation and if found to be in violation judges are empowered "to act 'proportionally' but 'with any means' to halt their dissemination."<sup>[44]</sup> In addition to a reporting system, the law obligates social media firms to cooperate with takedown orders and provide tools that flag misinformation. Finally, it empowers French broadcast regulators to ensure compliance and revoke the broadcast rights of television and radio news networks.<sup>[45]</sup> Since 2018, France has expanded its legal framework for managing misinformation by, for example, obligating social media firms to delete certain types of content with as little as one hour's notice.<sup>[46]</sup>

In conjunction with an aggressive domestic policy regime to manage misinformation, the French military is vigorously integrating information operations and cyber operations. While France's 2018 Offensive Cyber Doctrine focused primarily on cyberspace operations without extensive discussion of their link to information operations,<sup>[47]</sup> the October 2021 doctrinal publication "Éléments Public De Doctrine Militaire De Lutte Informatique D'influence" emphasizes the role of information operations. Integrating military and non-military disciplines such as the social sciences, the doctrinal statement centers "information space" operations on countering adversary information campaigns.<sup>[48]</sup> This new doctrinal focus on information operations complements the French Ministry of Defense's efforts to expand existing cyber forces.<sup>[49]</sup>

France's strong domestic policy regime and recent expansions of information and cyber forces make more challenging discerning the French military's role in countering foreign disinformation campaigns. Yet France is the only Western democracy credited by Facebook with running a coordinated disinformation campaign using its website. In December 2020 Facebook reported that it had taken down a network of French-linked Facebook accounts that had been waging a coordinated disinformation campaign in Mali and the Central African Republic to counter a disinformation campaign funded by a Russian oligarch.<sup>[50]</sup> This is one of the few known instances of contemporary offensive cyber-enabled information operations attributed to a Western democracy.

### ***Germany***

Overall, Germany has faced comparatively fewer foreign information threats,<sup>[51]</sup> with disinformation around the recent election coming largely from domestic sources.<sup>[52]</sup> Similar to France, in 2017 Germany enacted a law to strengthen regulation of social media content. However, this law focused primarily on enforcing take-down requirements for hate speech and other abusive content, but unlike the French law, is less directed against foreign-led coordinated disinformation campaigns.<sup>[53]</sup>

Germany's military response is led by the Cyber and Information Domain Service which was established in 2017. The service combines offensive cyber, electronic warfare, and information activities in one organization.<sup>[54]</sup> Additionally, in September 2021 Germany adopted a new cybersecurity strategy that emphasized the link between information and cyber operations.<sup>[55]</sup> However, given the relative newness of the command combined with the fact that Germany has previously prioritized defensive over offensive cyber efforts, there is little available knowledge of offensive German information or cyber operations.

### ***Russia's Invasion of Ukraine***

The 2022 Russian invasion of Ukraine will serve as a key event for evaluating the role of cyber-enabled information operations and democratic responses. However, at the time of writing in Spring 2022, the invasion remained in its early stages yet certain preliminary

observations can be made since information operations are ongoing. First, social media and Internet infrastructure firms have been extremely proactive in restricting and banning Russian users and in particular Russian state media outlets.<sup>[56]</sup> This may eventually lead to the creation of a de facto authoritarian internet as Russia responds by on-shoring internet infrastructure and increasing the scope of state censorship.<sup>[57]</sup> Second, the US and UK chose a risky public diplomacy strategy—traditional informational operations—in the run-up to the invasion by publicly messaging about Russia’s invasions plans in hopes of disrupting them.<sup>[58]</sup> To help shape narratives on social media, the White House also briefed social media influencers.<sup>[59]</sup> Finally, Ukraine seems to have won the perception war on social media—for now—through the creative use of memes and gripping first-person narratives to shape global public opinion in their favor.<sup>[60]</sup> These preliminary observations suggest that private firms and democracies have been much more proactive in shaping the information environment in the run-up the invasion.

### ***Offensive Cyber-enabled Information Operations by Democracies***

The previous section briefly summarizes how powerful Western democracies recently have steadily integrated offensive cyber and information operations in both doctrine and organization, giving comparatively little attention to how and whether to use cyber-enabled information operations. As democracies further integrate disciplines necessary for information operations into their cyber forces, there will be an increasing temptation and capacity to use offensive cyber-enabled information operations. There has been little public or scholarly debate over the costs and benefits of employment by democracies of offensive cyber-enabled information operations. This section first outlines how the US pioneered cyber-enabled information operations. Second, it discusses three tensions which democracies must contend with if they are to practice offensive information operations: Internet fragmentation, threats to democratic norms, and blowback.

### ***The United States as Democracy’s Pioneer of Offensive Cyber-Enabled Information Operations***

While the US engaged in psychological warfare and information operations throughout the War on Terror and Iraq War, these operations were more closely tied to specific military objectives.<sup>[61]</sup> One of the first instances of large-scale social media manipulation was conducted by the US against Cuba to promote a democratic revolution. More recently, inspired by the role Twitter played in Iran’s 2009 Green Movement, the U.S. Agency for International Development (USAID) leveraged a stolen database of Cuban cell phone numbers to create an SMS-based Twitter-like social network called ZunZuneo, which was designed to foment anti-regime activity:

the US government planned to build a subscriber base through “non-controversial content:” ... Later when the network reached a critical mass of subscribers, perhaps hundreds of thousands, operators would introduce political content aimed at inspiring Cubans to

organize “smart mobs” – mass gatherings called at a moment’s notice that might trigger a Cuban spring, or, as one USAID document put it, “renegotiate the balance of power between the state and society.”<sup>[62]</sup>

A key component of the program was profiling and studying the Cuban ZunZuneo subscriber base by assessing political loyalty and openness to revolution. The goals were to “move more people toward the democratic activist camp without detection” and help organize anti-regime “smart mobs.” ZunZuneo reached 40,000 Cuban subscribers by early 2011, but USAID ultimately shut-off the service in 2012.<sup>[63]</sup> USAID’s role in the platform was obfuscated through complicated contracting relationships, and ZunZuneo’s website had fake advertising placements to render it more authentic. ZunZuneo and USAID ties were not publicly revealed until a 2014 Associated Press report and later congressional investigations.<sup>[64]</sup>

Other instances of social media manipulation were the product of attempts to reduce terrorist recruitment in Afghanistan and the Middle East. For example, in 2011 it was revealed by the Guardian that the US military had contracted for a platform to manage fake social media persona as part of *Operation Earnest Voice*, to counter online recruitment by terrorist organizations and the Taliban.<sup>[65]</sup> In testimony to Congress, U.S. General James Mattis described their goal thusly: “we challenge their propaganda. We disrupt the recruiting... We bring out the moderate voices. We amplify those. And in more detail, we detect and we flag if there is adversary, hostile, corrosive content in some open-source Web forum, [and] we engage with the Web administrators to show that this violates Web site provider policies.” Responding to criticism of this program, Mattis argued “in today’s changing world, these are now traditional military activities. They’re no longer something that can only be handled by Voice of America or someone like that.”<sup>[66]</sup> Together, these demonstrate the extent to which the US helped pioneer offensive cyber-enabled information operations with either the goal of spreading democracy or reducing the reach of terrorist recruiters. However, the recent rapid expansion of these capabilities by the US and other Western democracies demands careful consideration of impacted democratic values.

### ***Tensions over Democratic use of Offensive Cyber-enabled Information Operations***

Democracies far more than autocracies depend on vibrant information ecosystems to enable democratic debate and accountability. The expansion of the democratic use of offensive cyber-enabled information operations brings with it a host of potential issues that challenge the open Internet and risk further eroding the trust of democratic publics in shared sources of information. This section flags three sources of tension that arise from the democratic embrace of cyber-enabled information operations: first, further Internet fragmentation; second, threats to democratic norms; and finally, information blowback against democratic societies.

Tensions over misinformation and information operations play a key role in accelerating the fragmentation of the Internet and the rise of a “cyber-Westphalia.” While some scholars believe that the Internet fragmenting into democratic vs authoritarian networks would be

a positive development,<sup>[67]</sup> that also would undermine certain benefits of the original cyberspace framework.<sup>[68]</sup> The reality and perception of information operations was a key driver in the early 2010's push towards greater Internet fragmentation. Chinese and Russian decision-makers viewed the Arab Spring and other political upheavals of the late 2000's/early 2010's as evidence of a novel information warfare threat from the West, and, in particular, the US.<sup>[69]</sup> While there is no evidence that these upheavals were the product of a US or otherwise Western subversion campaign, the US did aggressively intervene to maintain information flows during the Arab Spring by, for example, having the Voice of America dynamically alter content to defeat web filtering.<sup>[70]</sup> These efforts to circumvent content filtering combined with the social media manipulation in Operation Earnest Voice contributed to the threat perception of Russian and Chinese decision-makers. Over the next few years, both countries increased their censorship and perception shaping activities—notably with Russia creating a censorship regime akin to China's "Great Firewall."<sup>[71]</sup> The reaction of France and Germany to information operations—creating or intensifying social media censorship regimes—thus mirrors the earlier actions of Russia and China. Moreover, democratic censorship of disinformation vectors risks increasing Internet fragmentation by prompting a tit-for-tat dynamic. For example, when YouTube deleted several German-language channels run by Russia Today for engaging in COVID disinformation, Russia threatened to block YouTube entirely.<sup>[72]</sup> Sadly, this threat suggests that Internet fragmentation may occur even if democracies avoid because even defensive measures invite retaliation.

The second tension over democratic offensive information operations is potential threats to democratic norms. Discussing the revelations surrounding the French disinformation campaign in Mali and the Central African Republic the French researcher Alexandre Papae-manuel comments that: "... to become tougher, should democracies follow the example of authoritarian regimes?... It's a slippery slope."<sup>[73]</sup> Core democratic norms include freedom of expression and maintaining an information-rich civil society. Offensive cyber-enabled information operations threaten these norms by expanding the government's role in shaping the information environment using methods that are not clearly attributable. This risks both the normative claims that democracies make about their values to the rest of the world as well as the existence of free and open information ecosystems at home. At the same time that the French military was conducting cyber-enabled information operations in Africa, the French government issued a report cautioning against offensive actions.<sup>[74]</sup> An anonymous European disinformation researcher, commenting on the French campaign, remarked that "You can't complain that Russia is doing this sort of thing, and then turn around and do it yourself."<sup>[75]</sup> Democracies risk the charge of hypocrisy as different parts of their governments work at cross purposes—some trying to maintain a free and open information ecosystem while others seek to shape perception.

The final tension for the democratic use of offensive information operations is blowback: the unintended consequences that may arise from expanding offensive information capabilities. Western democracies are the home to many private cyber security and surveillance firms that have been implicated in human rights abuses and play a significant contracting role in the provisioning of cyber security.<sup>[76]</sup> A similar pattern is emerging in information operations and social media disinformation with the rapid rise of firms located in Western democracies offering “disinformation for hire.” These firms have been implicated in social media disinformation campaigns in 48 countries worldwide with operations ranging from coronavirus disinformation to targeting elections.<sup>[77]</sup> At the same time that these firms expand international operations, Western democracies such as the UK, US, and Germany have been wracked by large-scale domestic disinformation campaigns targeting elections led by public relations firms and politicians.<sup>[78]</sup> The embrace by democracies of offensive information operations risks expanding and deepening the network of private actors conducting disinformation campaigns. Another blowback risk is increasing cynicism about the trustworthiness of news in democratic societies. Many democracies already face declining levels of trust in news media<sup>[79]</sup> and social media firm’s algorithmic curation and content moderation has been frequently attacked as partisan in the US.<sup>[80]</sup> This decline in trust extends to interactions among social media users, with those accused of being a “Russian bot” becoming a common practice in anglophone social media.<sup>[81]</sup> Thus, offensive use of information operations by democracies risks increasing this distrust by deepening the perceived partisan bias of social media firms and new media and decreasing social trust. Taken together, the expansion of firms specializing in disinformation and the declining trust in social and news media institutions creates unique risks for democracies that depend on a trusted and vibrant information ecosystem, and they undermine the potential for the development of international norms that could restrain authoritarian misinformation campaigns.

## CONCLUSION

Despite the rush of democracies to overtly embrace cyber-enabled information operations in their military organizations and doctrine, there has been little evaluation of whether the democratic employment of these operations for offensive purposes is useful or desirable. This article sought to lay out a broader overview of the terrain of democratic offensive information operations to help create a foundation for this debate and in so doing, identify key tensions in the democratic use of these operations.

Should democracies employ offensive cyber-enabled information operations? This article concludes that the risks of conducting these operations outweigh their benefits. Globally, democracies are at a critical impasse with declining trust in democratic institutions and a seeming reversal in their expansion and consolidation. One element of this democratic decline is the increasing cynicism towards democratic institutions, debate, and news media.<sup>[82]</sup> The offensive employment of information operations risks deepening the challenges that democracies currently face. Instead, democracies should pursue two strategies: first, domestic regulation of “disinformation for hire” firms that specialize in private social media shaping and information operations. Proliferation of these firms seriously threatens the viability of democratic information ecosystems that would help counter charges of hypocrisy. Second, democracies should employ denial strategies against actors conducting offensive information operations.<sup>[83]</sup> More important than shaping partisan narratives in their favor, democracies should deter or compel adversaries by reducing their ability to conduct these operations. 🛡️

## NOTES

1. Larry Jay Diamond and Marc F. Plattner, *Liberation Technology: Social Media and the Struggle for Democracy* (Baltimore: Johns Hopkins University Press, 2012); Ryan Kiggins, “Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era,” *International Studies Perspectives* 16, no. 1 (2015): 86–105; Daniel McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and Internet* (London: Palgrave Macmillan, 2015).
2. Eric Lipton, David Sanger, and Shane Scott, “The Perfect Weapon: How Russian Cyberpower Invaded the U.S.,” *The New York Times*, December 13, 2016.
3. Camille Francois and Herb Lin, “The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot,” *Journal of Cyber Policy* 6, no. 1 (February 2021): 9–30. Sarah Kreps. *Social Media and International Relations* (Cambridge: Cambridge University Press, 2020).
4. For an extended discussion of what makes cyber-enabled information operations unique, see: Herbert Lin and Jaelyn Kerr, “On Cyber-Enabled Information Warfare and Information Operations,” in *Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford: Oxford University Press, 2021).
5. Kreps, *Social Media, and International Relations*, 25–26. Henry Farrell and Bruce Schneier, “Common-Knowledge Attacks on Democracy.,” *Berkman Klein Center* 2018-7 (2018).
6. Poynter, “A Guide to Anti-Misinformation Actions around the World,” *Poynter*, August 14, 2019, <https://www.poynter.org/ifcn/anti-misinformation-actions/>.
7. Michael Warner, “Invisible Battlegrounds: On Force and Revolutions, Military and Otherwise,” in *Palgrave Handbook of Security, Risk, and Intelligence*, ed. Robert Dover (London: Palgrave Macmillan, 2018), 256.
8. Laura Rosenberger, “Making Cyberspace Safe for Democracy,” *Foreign Affairs*, January 25, 2021, <https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy>.
9. Farrell and Schneier, “Common-Knowledge Attacks on Democracy.”
10. Kiggins, *Open for Expansion*.
11. Vincent Mosco. *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge: MIT Press, 2005).
12. Michael Warner, “The Character of Cyber Conflict,” *Texas National Security Review*, September 17, 2020, <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>.
13. Ryan Fedasiuk, “A Different Kind of Army: The Militarization of China’s Internet Trolls,” *Jamestown Foundation*, April 12, 2021, <https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls/>; Adrian Chen, “The Agency,” *The New York Times Magazine*, June 2, 2015, <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>; Elsa Kania, in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (Abingdon: Taylor & Francis Group, 2021), 46–53.
14. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012); Adam P. Liff, “Cyberwar: A New ‘Absolute Weapon’? the Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies* 35, no. 3 (2012): 401–428; Timothy J. Junio, “How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate,” *Journal of Strategic Studies* 36, no. 1 (2013): 125–133.; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2018); Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013); Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).; Nadiya Kostyuk, and Yuri Zhukov, “Invisible Digital Front: Can Cyber Events Shape Battlefield Events?” *Journal of Conflict Resolution*, 63, no. 2 (2019): 317–347.
15. Richard J. Harknett, and Max Smeets. “Cyber Campaigns and Strategic Outcomes.” *Journal of Strategic Studies*, *Journal of Strategic Studies*, 2020-03, 1–34; Robert Chesney, and Max Smeets, “Introduction: Is Cyber Conflict an Intelligence Contest?” *Texas National Security Review* 3, no. 4 (2020). <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>; Jon R. Lindsay, “Military Organizations, Intelligence Operations, and Information Technology,” *Texas National Security Review* 3, no. 4 (2020), <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>; Joshua Rovner, “What Is an Intelligence Contest?” *Texas National Security Review*, *Texas National Security Review*, 3, no. 4 (2020-09-17), <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>; Michael Warner, “The Character of Cyber Conflict.” *Texas National Security Review* 3, no. 4 (2020), <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>; Michael Poznansky, “Covert Action, Espionage, and the Intelligence Contest in Cyberspace.,” *War on the Rocks* (2021), <https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/>; Benjamin Jensen, “The Cyber Character of Political Warfare,” *Brown Journal of World Affairs* XXIV, no. 1 (2017): 157–171.

NOTES

16. Martin Libicki, “The Convergence of Information Warfare,” in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte and A. Trevor Thrall (Abingdon: Taylor & Francis, 2021), 15-27.; Mark Pomerleau, “More Work Needed to Integrate Cyber and Information Ops, Former Official Says,” C4ISRNet, March 6, 2021, <https://www.c4isrnet.com/information-warfare/2021/03/05/more-work-needed-to-integrate-cyber-and-information-ops-former-official-says/>; Herbert Lin, “Election Hacking, as We Understand It Today, Is Not a Cybersecurity Issue,” *Lawfare*, October 31, 2019, <https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue>.
17. Francois and Lin, *The Strategic Surprise of Russian information operations*, 16.
18. Ryan Shandler et al., “Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment,” *British Journal of Political Science*, 2021, 1-19; Sarah Kreps and Jacquelyn Schneider, “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics,” *Journal of Cybersecurity* 5, no. 1 (2019).
19. Rosenberger, *Making Cyberspace Safe for Democracy*.
20. Christopher Whyte, “How Deep the Rabbit Hole Goes: Escalation, Deterrence, and the ‘Deeper’ Challenges of Information Warfare in the Age of the Internet,” in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (Abingdon: Taylor & Francis, 2021), 238-245.
21. Brian M Mazanec and Patricia Shamai, “Stigmatizing Cyber and Information Warfare: Mission Impossible?,” in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Thrall, and Brian Mazanec (Abingdon: Taylor & Francis, 2021), 230-238.
22. Rosenberger, *Making Cyberspace Safe for Democracy*.
23. “The Honest Ads Act.” Office of U.S. Senator Mark R. Warner, May 2019, <https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act>.
24. “Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System,” Justice News. Department of Justice, February 16, 2018, <https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere>.
25. Andy Greenberg, “US Hits Russia with Biggest Spying Retaliation ‘since the Cold War,’” *Wired*, December 29, 2016, <https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/>.
26. Karoun Demirjian, “Senate Overwhelmingly Passes New Russia and Iran Sanctions,” *The Washington Post*, June 15, 2017, [https://www.washingtonpost.com/powerpost/senate-overwhelmingly-passes-new-russia-and-iran-sanctions/2017/06/15/df9afc2a-51d8-11e7-91eb-9611861a988f\\_story.html](https://www.washingtonpost.com/powerpost/senate-overwhelmingly-passes-new-russia-and-iran-sanctions/2017/06/15/df9afc2a-51d8-11e7-91eb-9611861a988f_story.html).
27. Francois and Lin, *The Strategic Surprise of Russian Information Operations*.
28. Air Force, *AFDD 3-12 Cyberspace Operations* (Washington, DC: Air Force, 2011).
29. Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations 2018* (Washington, DC: Chairman JCS, 2018), ix.
30. Gina Harkins, “Fake News Is Wreaking Havoc on the Battlefield. Here’s What the Military’s Doing About It,” *Military.com*, August 17, 2020, <https://www.military.com/daily-news/2020/08/16/fake-news-wreaking-havoc-battlefield-heres-what-militarys-doing-about-it.html>.
31. Herbert Lin, “Doctrinal Confusion and Cultural Dysfunction in the Pentagon over Information and Cyber Operations,” *Lawfare*, March 31, 2020, <https://www.lawfareblog.com/doctrinal-confusion-and-cultural-dysfunction-pentagon-over-information-and-cyber-operations>.
32. Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” *The Washington Post*, February 27, 2019, [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](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).
33. Harkins, “Fake News Is Wreaking Havoc on the Battlefield.”
34. Brandi Vincent, “The Marines Are Copying the Air Force’s Efforts to Counter Online Disinformation,” *Defense One*, September 14, 2021, <https://www.defenseone.com/threats/2021/09/military-intel-officials-highlight-efforts-counter-online-disinformation/185346/>.
35. Heather Burns, “Why the Online Safety Bill Threatens Our Civil Liberties,” *Politics.co.uk*, May 27, 2021, <https://www.politics.co.uk/comment/2021/05/26/why-the-online-safety-bill-threatens-our-civil-liberties/>.
36. BBC, “Fake News and How to Spot It to Be Taught in Schools - CBBC Newsround,” *BBC News*, July 15, 2019, <https://www.bbc.co.uk/newsround/48988778>.

## NOTES

37. Ministry of Defense, *Cyber Primer*, (London: Ministry of Defense, 2016), 59.
38. Peter Walker, "New National Security Unit Set up to Tackle Fake News in the UK," *The Guardian*, January 23, 2018, <https://www.theguardian.com/politics/2018/jan/23/new-national-security-unit-will-tackle-spread-of-fake-news-in-uk>.
39. Dan Sabbagh, "Army Fights Fake News with Propagandists and Hackers in One Unit," *The Guardian*, July 31, 2019, <https://www.theguardian.com/technology/2019/jul/31/army-fights-fake-news-with-propagandists-and-hackers-in-one-unit>.
40. "National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK," [gchq.gov.uk](https://www.gchq.gov.uk), November 19, 2020, <https://www.gchq.gov.uk/news/national-cyber-force>; HM Government, *National Cyber Strategy 2022*, (London: HM Government, 2022), 59.
41. Jeremy Fleming, "Director's Speech at Cyber UK 2018," [gchq.gov.uk](https://www.gchq.gov.uk), April 12, 2018, <https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018>.
42. Mark Hookham, "Troops Face New Enemy - Kremlin's Fake News," *The Sunday Times*, March 18, 2017, <https://www.thetimes.co.uk/article/troops-face-new-enemy-kremlins-fake-news-q0dbnfq79>.
43. Helen Warrell, "UK on High Alert for Anti-Vaccine Disinformation from Hostile States," *The Financial Times*, December 11, 2020, <https://www.ft.com/content/7502f1f1-e104-403d-975f-bede6e518fe2>.
44. Alexander Ricci, "French Opposition Parties Are Taking Macron's Anti-Misinformation Law to Court," *Poynter*, September 30, 2019, <https://www.poynter.org/fact-checking/2018/french-opposition-parties-are-taking-macrons-anti-misinformation-law-to-court/>.
45. *Ibid.*
46. Simon Chandler, "French Social Media Law Is Another Coronavirus Blow to Freedom of Speech," *Forbes*, May 14, 2020, <https://www.forbes.com/sites/simonchandler/2020/05/14/french-social-media-law-is-another-coronavirus-blow-to-freedom-of-speech/>.
47. Arthur Laudrain, "France's New Offensive Cyber Doctrine," *Lawfare*, October 31, 2019, <https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine>.
48. Lukasz Olejnik, "French Doctrine of Information Operations - Engaging over Information Space," *Security, Privacy & Tech Inquiries*, October 22, 2021, <https://blog.lukaszolejnik.com/french-doctrine-of-information-operations-engaging-over-information-space/>.
49. AFP, "France To Boost Cyber Warfare Force," *Barrons*, September 8, 2021, <https://www.barrons.com/news/france-to-boost-cyber-warfare-force-01631123408>.
50. Facebook, "Removing Coordinated Inauthentic Behavior from France and Russia," Facebook Newsroom, December 2020, <https://about.fb.com/news/2020/12/removing-coordinated-inauthentic-behavior-france-russia/>.
51. Jeffrey Mankoff, "Russian Influence Operations in Germany and Their Effect," *Center for Strategic and International Studies*, December 17, 2020, <https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect>.
52. Jessica Bateman, "Germany Braces for Election Disinformation," *Foreign Policy*, September 13, 2021, <https://foreignpolicy.com/2021/09/13/germany-election-disinformation-social-media/>.
53. Poynter, "A guide to anti-misinformation actions around the world," *Poynter*, August 14, 2019, <https://www.poynter.org/ifcn/anti-misinformation-actions/>.
54. Council on Foreign Relations, "Germany Develops Offensive Cyber Capabilities without a Coherent Strategy of What to Do with Them," *Council on Foreign Relations*, December 3, 2018, <https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them>.
55. "The Federal Government Has Adopted the Cyber Security Strategy," *Website of the German Federal Government*, September 8, 2021, <https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688>.
56. Mark Scott and Rebecca Kern, "Social Media Goes to War," *Politico*, March 3, 2022, <https://www.politico.eu/article/social-media-goes-to-war/>.
57. Steven Vaughan-Nichols, "Russia may be cutting itself off from the internet," *ZDNet*, March 10, 2022, <https://www.zdnet.com/article/russia-may-be-cutting-itself-off-from-the-internet/>.
58. Max Colchester and Warren Strobel, "U.S., Allies Fight Information War with Russia to Deter Ukraine Invasion," *The Wall Street Journal*, <https://www.wsj.com/articles/u-s-allies-fight-information-war-with-russia-to-deter-ukraine-invasion-11644402601>.

NOTES

59. Taylor Lorenz, “The White House is Briefing TikTok Stars about the war in Ukraine,” *The Washington Post*, March 11, 2022, <https://www.washingtonpost.com/technology/2022/03/11/tik-tok-ukraine-white-house/>.
60. Anjana Susaria, “Why Zelenskyy’s ‘selfie videos’ are helping Ukraine win the PR war against Russia,” March 1, 2022, <https://theconversation.com/why-zelenskyy-s-selfie-videos-are-helping-ukraine-win-the-pr-war-against-russia-178117>; Lizzie O’Leary, “Ukraine is Winning the Information War With Russia,” *Slate*, March 4, 2022, <https://slate.com/technology/2022/03/ukraine-is-winning-the-information-war-with-russia.html>.
61. Ross Caputi, “The Troubling Legacies of U.S. Information Operations during the Iraq Occupation,” Scholars Strategy Network, January 11, 2018, <https://scholars.org/contribution/troubling-legacies-us-information-operations-during-iraq-occupation>.
62. Associated Press, “US Secretly Created ‘Cuban Twitter’ to Stir Unrest and Undermine Government,” *The Guardian*, April 3, 2014, <https://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest>.
63. Associated Press, “US Secretly Created ‘Cuban Twitter’ to Stir Unrest and Undermine Government.”
64. Bernard E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015), 8-10.
65. Nick Fielding and Ian Cobain, “Revealed: US Spy Operation That Manipulates Social Media,” *The Guardian*, March 17, 2011, [https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks?CMP=share\\_btn\\_tw](https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks?CMP=share_btn_tw).
66. Walter Pincus, “New and Old Information Operations in Afghanistan: What Works?” *The Washington Post*, March 28, 2011, [https://www.washingtonpost.com/world/new-and-old-information-operations-in-afghanistan-what-works/2011/03/25/AFxNAeqB\\_story.html](https://www.washingtonpost.com/world/new-and-old-information-operations-in-afghanistan-what-works/2011/03/25/AFxNAeqB_story.html).
67. Rosenberger. “Making Cyberspace Safe for Democracy.”
68. Chris Demchak, “Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age,” *The Cyber Defense Review* 5, no. 1 (2016): 49-51.
69. Keir Giles, *Handbook of Russian Information Warfare* (Rome, Italy: NATO Defence College Research Division, 2016), 36-44; Warner, “The Character of Cyber Conflict.”
70. McCarthy 2015, 119–121.
71. Ryan Fedasiuk, “A Different Kind of Army: The Militarization of China’s Internet Trolls,” Jamestown Foundation, April 12, 2021, <https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls/>; Fedasiuk 2021. Lincoln Pigman, “Russia’s Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion,” *Journal of Cyber Policy* 4, no. 1 (2018): 23-24.
72. Rachel Pannett, “Russia Threatens to Block YouTube after German Channels Are Deleted over Coronavirus Misinformation,” *The Washington Post*, September 29, 2021, <https://www.washingtonpost.com/world/2021/09/29/russia-ban-youtube-german-coronavirus/>.
73. Quoted in AFP, “France Struggling in Sahel ‘Information War,’” *France 24*, February 11, 2021, <https://www.france24.com/en/live-news/20210211-france-struggling-in-sahel-information-war>.
74. Mark Scott and Elisa Braun, “France Feuds with Facebook over Disinformation Claims,” *Politico*, December 17, 2020, <https://www.politico.eu/article/france-facebook-disinformation/>.
75. Ibid.
76. Sidney Fussell, “French Spyware Executives Are Indicted for Aiding Torture,” *Wired*, June 23, 2021, <https://www.wired.com/story/french-spyware-executives-indicted-aiding-torture/>; Tim Shorrocks, “How Private Contractors Have Created a Shadow NSA,” *The Nation*, December 30, 2019, <https://www.thenation.com/article/archive/how-private-contractors-have-created-shadow-nsa/>.
77. Samantha Bradshaw, Hannah Bailey, and Philip Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: Project on Computational Propaganda, 2021), i.
78. Jane Lytvynenko, “In 2020, Disinformation Broke the US,” BuzzFeed News, April 14, 2021, <https://www.buzzfeednews.com/article/janelytvynenko/disinformation-broke-us>; Isaac Stanley-Becker, “Pro-Trump Youth Group Enlists Teens in Secretive Campaign Likened to a ‘Troll Farm,’ Prompting Rebuke by Facebook and Twitter,” *The Washington Post*, September 16, 2020, [https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c\\_story.html](https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c_story.html); Adam Satariano and Amie Tsang, “Who’s Spreading Disinformation in U.K. Election? You Might Be Surprised,” *The New York Times*, December 10, 2019, <https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html>.

NOTES

79. Michael Schudson, "The Fall, Rise, and Fall of Media Trust," *Columbia Journalism Review*, 2019, [https://www.cjr.org/special\\_report/the-fall-rise-and-fall-of-media-trust.php](https://www.cjr.org/special_report/the-fall-rise-and-fall-of-media-trust.php); Benjamin Toff et al., "Overcoming Indifference: What Attitudes towards News Tell Us about Building Trust," Reuters Institute for the Study of Journalism, September 9, 2021, <https://reutersinstitute.politics.ox.ac.uk/overcoming-indifference-what-attitudes-towards-news-tell-us-about-building-trust>.
80. Emily Vogels, Andrew Perrin, and Monica Anderson, "Most Americans Think Social Media Sites Censor Political Viewpoints," Pew Research Center: Internet, Science & Tech (Pew Research Center, September 18, 2020), <https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/>.
81. Hanna Kozłowska, "Russian Trolls and Bots Are Successful Because We Know They Exist," Quartz, January 30, 2020, <https://qz.com/1792155/russian-trolls-and-bots-are-successful-because-we-know-they-exist/>.
82. Yascha Mounk, "Democracy on the Defense," *Foreign Affairs*, March 1, 2021, <https://www.foreignaffairs.com/articles/united-states/2021-02-16/democracy-defense>; "The Global Democratic Recession. And How to Reverse It" with Larry Diamond," Indiana University, December 6, 2020, [https://iu.mediaspace.kaltura.com/media/%E2%80%9CThe+Global+Democratic+Recession.+And+How+to+Reverse+It%E2%80%9D+with+Larry+Diamond/1\\_gfca8m0v](https://iu.mediaspace.kaltura.com/media/%E2%80%9CThe+Global+Democratic+Recession.+And+How+to+Reverse+It%E2%80%9D+with+Larry+Diamond/1_gfca8m0v).
83. Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, March 2021, 1-36.



# Between Two Stools: Military and Intelligence Organizations

*in the Conduct  
of Offensive  
Cyber Operations*

---

Ewan Lawson

From 2018, members of the coalition fighting against the Islamic State in Iraq and Syria confirmed that they had been conducting offensive cyber activities as part of the campaign in an operation given the codename GLOWING SYMPHONY.<sup>[1]</sup> While the details of these operations largely remain highly classified, they are the first example of states publicly admitting to such operations during armed conflict. They are also notable as while Fleming in his speech cited above emphasized that the UK effort resulted from cooperation between its signals intelligence (SIGINT) agency GCHQ and the Ministry of Defence (MOD), one of the other partners, Australia, emphasized the role of civilian personnel from its SIGINT organization, the Australian Signals Directorate.<sup>[2]</sup> This was arguably the first public recognition of the extent to which, at least in some states, intelligence organizations and the military were entwined in the conduct of contemporary offensive cyber operations.

This integration is likely to be a feature of future offensive cyber operations. In October 2021, it was revealed that the UK's National Cyber Force (NCF), which includes intelligence officers, military personnel, and law enforcement, was conducting such operations against actors involved in a series of ransomware attacks, providing further evidence of a blurring of the actors involved in offensive activities in cyberspace.<sup>[3]</sup>

While it is recognized that this is taking place partly in response to some states deliberately making use of organized crime groups or civilian so-called: patriotic hackers, this article argues that the blurring of responsibilities between intelligence agencies and the



**Ewan Lawson** is an independent researcher on defence and security issues having previously been a Senior Research Fellow at the Royal United Services Institute. He is also a Teaching Fellow at the School of Oriental and African Studies at the University of London and has been engaged by the International Committee of the Red Cross, to examine military cyber operations and international humanitarian law.

He researches a range of subjects including cyber security, strategy and cross-government working, military influence and information operations, law of armed conflict and war crimes, and conflict in Africa.

He was previously a Royal Air Force officer, completing joint warfare appointments including tours as a joint operational planner, as the commander of the UK Psychological Operations Group, as faculty at both the UK and Kuwait Staff Colleges and as Defence Attaché in South Sudan. He also worked on the development of UK cyber warfare capabilities.

military in the conduct of offensive cyber operations is problematic and that there is a need for deliberate organizational and operational distinction. What is, in effect, the para-militarization of operations in cyberspace has the clear potential to contribute to instability in the international system in two main ways. First, it contributes to the risk of unexpected and unintended escalation through reinforcing the security dilemma for states subject to hostile intrusions. Second, it contributes to the growing space for disruptive and destructive operations below the level of armed conflict in the so-called “grey zone,” and hence outside the spaces where civilians can be protected under international humanitarian law (IHL).

The article first outlines the background of how this position has arisen. In doing so, it will focus on the states that declared their involvement in GLOWING SYMPHONY: the UK, Australia, and the US as cases. Having considered the organizational context, it then reviews whether there is something inherent in cyberspace that leads to what has been called an intelligence competition.<sup>[4]</sup> It next moves on to consider how the blurring of responsibilities in military cyber operations between intelligence organizations and the military might increase the risk of unforeseen escalation, and the implications of operations conducted below the level of armed conflict. Finally, it considers how states might address this issue.

In many states, intelligence agencies play a significant role in building capacity in both cyber security and offensive cyber operations. This reflects in part that those agencies have transitioned from traditional signals intelligence to also collecting data from digital sources. They have developed access to the networks of actual and potential adversaries, primarily for the purpose of intelligence collection but increasingly with an awareness of the potential to deliver both physical and cognitive effects through the addition, deletion, or manipulation of data on those networks.

As militaries became aware of this potential to deliver destructive or disruptive effects through offensive cyber activities during the conduct of operations, an inevitable linkage with the intelligence agencies in this field developed. Indeed, in some cases the signals intelligence agencies had their roots in, or indeed still were part of, the military. In the UK, GCHQ as the national SIGINT agency has taken the technical and operational lead in many aspects of cyber policy and formed the base around which the National Cyber Security Centre (NCSC) was established in 2016 as the focus for cyber security and national cyber defense.<sup>[5]</sup>

Over the last decade, the UK has reorganized its offensive cyber capabilities, culminating in the formation of the NCF in 2020. This seeks to bring together the operational experience of GCHQ and MOD along with the overseas-focused Secret Intelligence Service (SIS) and the research organization Defence, Science and Technology Laboratories (Dstl).<sup>[6]</sup> It builds upon a longer relationship between the military and GCHQ in SIGINT and a developing one in the conduct of offensive cyber operations. It is important to note that from its launch the NCF has been expected to operate against a range of targets, not just states and violent non-state actors but also criminal groups.<sup>[7]</sup>

Whereas in the UK, GCHQ reports to the Foreign, Commonwealth and Development Office (FCDO), the Australian Signals Directorate (ASD) has retained its roots as a statutory agency within Defence since 2017. Similarly, the US SIGINT elements, the National Security Agency (NSA), operates under the Department of Defense although its Director is “dual-hatted” as the military commander of U.S. Cyber Command (USCYBERCOM). This latter organization delivers cyber support, both offensive and defensive, to US military operations, although the regional combatant commanders that cover the globe also have cyber capabilities under their command.

It is important to recognize that many states’ intelligence agencies have a paramilitary aspect to their operations. In the examples of the UK and Australia, these sorts of activities are usually conducted by military personnel acting in support of the civil power. In the US, the Central Intelligence Agency (CIA) has had a paramilitary component since being formed at the end of World War II as the successor to the Office of Strategic Services (OSS).<sup>[8]</sup> The most visible contemporary manifestation of this is the undeclared campaign of targeted killings undertaken by drones as part of counterterrorism operations in places like Pakistan, Somalia, and Yemen. Although authors have questioned the extent to which these operations are compatible with domestic and international law, it seems likely that the use of paramilitary forces in conflicts that fall below the threshold of armed conflict will be part of future inter-state competition including in cyberspace.<sup>[9]</sup> This is already seen in USCYBERCOM’s strategic approach of persistent engagement which will be discussed later in this article.

As noted previously, it is important to recognize that this blurring of organizations involved in delivering effects in cyberspace is not unique to Western democracies. Indeed, the desire to respond to coercive activities conducted by adversaries and competitors in cyberspace below

the level of armed conflict is a significant driver in the development of these approaches. The relative anonymity provided by cyberspace has encouraged states to take the opportunity this provides to operationalize coercive strategies using actors including organized crime groups and “patriotic hackers” with the intention of distancing the state from the activity. The blurring described here between intelligence and military organizations is arguably less morally, ethically, and legally contentious but, as will be outlined, it has potentially similar impacts in terms of escalation risk and undermining IHL.

It can be seen that, at least in the three Western examples, the national structures designed to deliver offensive cyber capability involve a mix of civilian and military personnel, and capabilities from intelligence agencies and the military. At the heart of this combination is the challenge of gaining access to networks and systems whether for the purposes of gathering intelligence or delivering effects. This is an essential step in either form of operation and, indeed, reconnaissance of a target system is part of any offensive cyber “kill chain” process.<sup>[10]</sup> Given that the priority in the early stages of the digital revolution was on the opportunities for accessing and exploiting data, it is unsurprising that the intelligence agencies developed the skills necessary for identifying and exploiting such accesses.

Conceptually, academics and commentators frequently question whether traditional frameworks to describe war and conflict are appropriate when applied to cyberspace. One alternate framework recognizes the central role of intelligence agencies and suggests that it is better described as an intelligence contest.<sup>[11]</sup> At its heart, an intelligence contest is about stealing information from competitors and adversaries, protecting one’s own information, and disrupting the opponent’s data and communications. Rovner identifies five defining characteristics of an intelligence contest:<sup>[12]</sup>

- a. An effort to collect more and better information on adversaries’ capabilities and intentions.
- b. An effort to exploit any discovered information for practical gain such as decision advantage or to improve the balance of capabilities.
- c. An effort to undermine adversary morale, institutions, and alliances.
- d. An effort to disable adversary intelligence collection capabilities.
- e. A campaign to pre-position assets for future collection including in the event of armed conflict.

On this basis, Rovner argues that current competition in cyberspace is more reflective of an intelligence contest than being framed through the language of war and armed conflict.<sup>[13]</sup> On this basis, the central role for intelligence agencies in cyber operations seems logical. However, even Rovner recognizes that it does not quite cover the extent of offensive cyber operations, which also include military conflict and some forms of diplomacy.<sup>[14]</sup>

Critiques of this alternate way of conceptualizing conflict in cyberspace note both the kinship between intelligence operations and those in cyberspace, including covert paramilitary actions. However, rather than seeing intelligence operations as the central activity in cyberspace, instead note they are conducted in support of diplomacy, military operations, and internal security.<sup>[15]</sup> In particular, Warner argues that Rovner's five characteristics are representative of cyber operations in support of diplomacy and internal security but not military operations which are likely to be more destructive than merely disruptive.<sup>[16]</sup> While some would argue that the use of military language with regard to cyberspace operations is simply a way of achieving bureaucratic and budgetary advantage, the critique highlights the limitations of focusing on the intelligence contest approach.<sup>[17]</sup> This in turn highlights the potential for problems with the blurring of operations conducted by intelligence organizations as part of the contest and those conducted by the military as part of an armed conflict. But in what ways might those problems manifest in practice?

One of the key challenges links to the condition of uncertainty that exists in international politics.<sup>[18]</sup> In the international relations theory of defensive structural realism, the nature of the international system can give rise to the security dilemma. Defensive structural realists see states acting to secure themselves in an anarchic international system. It argues that states are fundamentally rational, and that conquest or military aggression is difficult given that the balance is in favor of the defense. It therefore argues that states should rationally seek to maintain the status quo and hence seek to balance against competitors.<sup>[19]</sup> While this theoretical framework can be effective at explaining response to coercive or aggressive activities by a state, it is less useful in explaining why states might choose those approaches. One possible explanation is the security dilemma in which states undertake policies designed to secure their own security, which either by design or unintentionally reduce the security of an adversary or at least its perception of security. In turn, the adversary may react to this perception by adopting policies that in turn decrease the security of the originator. In this way, conflicts can escalate, whatever the original intentions.<sup>[20]</sup> Ultimately, this is a dilemma of interpretation as well as a dilemma of response.<sup>[21]</sup>

Buchanan makes a compelling case for the applicability of the security dilemma to states' interactions in cyberspace.<sup>[22]</sup> In particular, he notes that operations which seek to collect information and gain intelligence, however conducted, can be threatening to the states against which they are conducted.<sup>[23]</sup> It does not matter if the intentions of the collecting state are relatively benign; it is the perception of the target that is key, along with the decision as to what is an appropriate response. Thus, in the Cold War, NATO aircraft flew toward the borders of the Warsaw Pact in order to collect both technical intelligence on radar systems but also on the nature of the response. Although this activity had an intent that was simply about collecting information, it ran the risk of being misinterpreted as part of an aggressive strike.

In cyberspace, the problem arises in the first instance when a defender detects that an actor has gained access to its network. While most computer network exploitation operations will be designed to go undetected, this clearly cannot be guaranteed, and to the target it is likely that it will at least initially be unclear as to the precise purpose of the intrusion. Thus, there is a clear risk of misperception potentially influenced by the wider political and security context at the time. Through technical analysis and the identification of patterns of use of tools, techniques, and infrastructure, it is possible to identify threat actors and link them to organizations including intelligence agencies, albeit with varying degrees of certainty. A target may be able therefore to make some deductions as to the purpose of the intrusion based on the identity of the threat actor.

The integration of intelligence agencies with the military in the conduct of offensive cyber operations could therefore easily lead to the misperception that an intrusion, conducted by the former for the purposes of exploitation, could be for disruptive or destructive purposes as part of a military campaign. Would this in and of itself necessarily be escalatory? It has been argued that “past cyber incidents are associated with limited escalation,”<sup>[24]</sup> but the evidence base is at present limited. It appears that escalation arising from competition and conflict in cyberspace may be more complex than the traditional model of a ladder or spiral. Given that the “linkages between intent, effect and perception are loose,”<sup>[25]</sup> it is possible that escalation may be as much horizontal, into other domains, as vertical and increasing the intensity of the conflict in cyberspace.<sup>[26]</sup> While the risk and indeed the nature of escalation arising from operations in cyberspace continue to not to be well understood and, given the limited evidence base to date, it would seem sensible to minimize that risk wherever possible, including reducing the risk of misinterpretation of the purpose of such operations.

One way in which some states perhaps have sought to minimize the risk of escalation is through coercive activities which are designed to stay below the level of a conventional military response. This so-called “hybrid warfare” has been enabled by the digital revolution and has included disruptive offensive cyber operations and digitally-enabled information operations. The continuing conflict in Ukraine has seen disruption of the power grid in Kyiv along with disinformation campaigns targeted at the population both in Ukraine itself and in friendly states.<sup>[27]</sup> It has also included cyber operations against military targets and a domestically developed app which improved the targeting of Ukrainian artillery but was hacked in order to provide location data that in turn allowed those formations to be attacked.<sup>[28]</sup> While it can be argued that hybrid activities taking place in Donbas are part of an armed conflict and therefore need to be conducted in accordance with the principles of IHL, it is less clear that an offensive cyber operation in Kyiv reaches that threshold.\*

The principles of IHL are designed to protect non-combatants during armed conflict, and states have broadly agreed at the UN that these apply to operations in cyberspace.<sup>[29]</sup> However, the International Committee of the Red Cross (ICRC) in a recent report raised concern

\*This article was written before the implications of the Russian invasion of Ukraine in February 2022 could be evaluated and hence refers to the period of conflict before that.

that states may have differing perspectives on the applicability of IHL to offensive cyber operations conducted in the context of hybrid warfare below the threshold of armed conflict.<sup>[30]</sup> While some have indicated that they would apply the principles of IHL to all offensive cyber operations which might impact civilians, this is far from universally agreed and remains a contentious issue. To an extent, the debate focuses on technical legal arguments around what constitutes an “attack” as defined in the Geneva Conventions when conducted in cyberspace, and whether “data” can be considered an object under IHL. However, it also reflects the broader discussion about operations conducted below the legal threshold of armed conflict and the need to protect civilians.<sup>[31]</sup>

Further, the ICRC report also raises concern about the role of intelligence agencies in the conduct of offensive cyber operations, noting that the authorities for conducting espionage or exploitation are in many states different from those enabling disruptive and destructive effects. Further, the report highlighted that the international norms and laws for managing armed conflict are considerably more developed than those for espionage. This raises concerns about how cyber operations that transit from exploitation to an offensive function are managed, particularly when it involves a transition of responsibility between an intelligence agency and the military.<sup>[32]</sup>

The current posture adopted by USCYBERCOM also blurs this line between intelligence collection and disruptive/destructive offensive cyber operations. DoD adopted a strategy known as “Defend Forward” which has been operationalized by USCYBERCOM through the doctrine of “Persistent Engagement”.<sup>[33]</sup> The intent is to identify, counter, and mitigate threats before they enter US networks or impact US interests. This requires the aggressive collection of intelligence which, coupled with the potential for such accesses to be developed into offensive cyber operations, raises again the risk of escalation through misinterpretation and the security dilemma. While this approach is designed to counter the potentially corrosive effects of activities such as election interference and is apparently conducted under appropriate national authorities and cognizant of international law, it once again blurs the distinction between intelligence operations and those designed to deliver effects, and are conducted by a military organization potentially below the threshold of armed conflict. Further, it has been argued that if Persistent Engagement is the focus of USCYBERCOM it risks a mindset that prioritizes aggressive tactics which might be appropriate in a period of relative peace when escalation is unlikely but might be counterproductive in a period of intense crisis or conflict. If these are the risks from the blurring of intelligence agencies and the military in cyberspace, what are the options?

This article does not seek to argue that states should not respond to coercive and aggressive activities in cyberspace. Indeed, it can be argued that although each has a different construct the approaches adopted in Australia, the UK, and the US in creating hybrid organizations balances the risk of blurring the legal frameworks for those cyber operations designed for exploitation and those for effect. While inevitably the detail of how they operate is opaque, there

is little doubt about the potential to ensure shared understandings across the organizations of responsibilities and authorities, and to manage the transitions between intelligence collection and effects operations in ways that minimize the risks of those responsibilities and authorities being misunderstood or misused. However, as this article argues, it also contributes to increasing the risk of misperception on the part of the target as to what is intended, which could in turn have unforeseen escalatory consequences. Therefore, what is the alternative?

States should consider how they create clear structural and practical distance between those organizations tasked with intelligence collection, and network exploitation for that purpose, and those that are tasked with delivering disruptive and destructive effects, whether cognitive or physical. This would contribute to reducing the risk of misperceptions as to the reasons behind a network intrusion when it is discovered by a target state and the initiating organization is identified or suspected. More research is required into the relationships between perceptions and escalation risk resulting from cyber operations, and the relative significance of factors such as the political context, the nature of the targeted system, and the potential identification of the type of organization conducting the operation. This research could be conducted through the analysis of real-world case studies as well as tabletop exercises conducted with practitioners.

In this way, an organization such as the NCF in the UK, while attractive in terms of potential operational and fiscal efficiencies, contributes to increasing the risk. Equally, given the continuing intensity of competition and conflict in cyberspace, it would be naïve to expect a successful cyber power not to seek to exploit and develop opportunities identified through intelligence operations. Therefore, there is a need to consider alternate organization models. For example, rather than creating an integrated organization, another approach would be to create a central coordination mechanism that would allow those organizations which need to conduct operations in cyberspace, whether for exploitation or to deliver effects, to focus on their areas of responsibility while ensuring that opportunities identified by agencies are not missed by others. This will, of course, always leave the debate in certain circumstances as to whether delivering an effect and hence potentially losing access and valuable intelligence is the right decision, but these options are ones that are best addressed by an organization that is separate from the bureaucratic interests of the various operators. It can make operational decisions based on a clear understanding of national strategy.

The US has had a more public discussion of some of these issues resulting in part from the leaks of material by Edward Snowden but also a complex interagency process which some have argued has impacted the ability of USCYBERCOM to respond to hostile cyber operations in a timely manner. These issues appear to have been addressed through the allocation of greater authority to the military, but it is not clear that this will reduce the risks highlighted in this article, and indeed it might intensify them.<sup>[34]</sup>

In conclusion, the blurring of actors in cyberspace continues to be a concern, whether referring to those states using non-state actors such as organized crime groups or “patriotic hackers,” or those such as Australia, the UK, and the US, which have sought to integrate military and civilian intelligence capabilities. While the latter is arguably necessary given the challenge of coercive activities in cyberspace and the benefits that would accrue from operational and fiscal efficiency, this article argues that it adds to the potential risks arising from this blurring.

In particular, the nature of cyberspace means that for states targeted it can be difficult to assess the purpose of an intrusion. This creates a potential security dilemma for those on the receiving end in terms of both perception and response. Although escalation risk from activities in cyberspace is still not well understood, the continuing integration of organizations with responsibility for exploitation and the delivery of effects increases the risk of misperception and unintended escalation. Further, offensive cyber operations below the level of armed conflict may not be conducted under the principles of IHL but potentially under legal frameworks designed for intelligence collection and exploitation. This potentially contributes to an increased risk of civilian harm arising from offensive cyber operations.

Future offensive cyber activities have the potential to be more disruptive and indeed destructive. While some states (often disingenuously) have called for the demilitarization of cyberspace or its being maintained as a venue for peaceful activities only, the offensive cyber genie is already out of the bottle. Instead, we should actively consider the extent to which contemporary thinking on offensive cyber is contributing to future risks; both to international peace and to our societies. Consideration needs to be given to whether the integration of intelligence and military cyber capabilities is the best approach in light of the risks and whether instead there is a need to create clear space between the different organizations within a state that have a legitimate reason to operate in cyberspace. The risks of unintended escalation and of civilian harm should outweigh the desire for perceived operational and fiscal efficiency.♥

**NOTES**

1. Jeremy Fleming, 2019, Speech at *Cyber UK 2018*, GCHQ, <https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018>.
2. Stephanie Borys, 2019 *Licence to Hack: Using a Keyboard to fight Islamic State*, ABC News Online, <https://www.abc.net.au/news/2019-12-18/inside-the-islamic-state-hack-that-crippled-the-terror-group/11792958?nw=0&r=HtmlFragment>.
3. Helen Warrell, 2021, "GCHQ to use new cyberforce to hunt ransomware gangs," *Financial Times*, <https://www.ft.com/content/2e391872-428d-44bf-8910-23f123c8aaa6>, accessed October 28, 2021.
4. Robert Chesney and Max Smeets, 2020, "Introduction: Is Cyber Conflict an Intelligence Contest" in: *Policy Roundtable: Cyber Conflict as an Intelligence Contest*. Austin: Texas National Security Review, <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>.
5. NCSC. n.d. *About the NCSC: What we do*, <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>, accessed September 13, 2021.
6. Joe Devanny, Andrew Dwyer, Amy Ertan, and Tim Stevens 2021, *The National Cyber Force that Britain Needs?* London: Kings College London, 7.
7. NCSC n.d.
8. D.H. Berger, 1995, *Use of Covert Paramilitary Activity as a Policy Tool: An analysis of Operations conducted by the US Central Intelligence Agency, 1949-51*, United States: Marine Corps Command and Staff College, <https://www.hsdl.org/?abstract&did=445885>.
9. Sterio, Milena. 2018. "Lethal Use of Drones: When the Executive is Judge, Jury and Executioner," *The Independent Review*, Vol. 23 No. 1, 35-50.
10. Christopher Whyte and Brian Mazanec, 2019, *Understanding Cyber Warfare: Politics, Policy and Strategy*, London: Routledge, 93.
11. Chesney and Smeets, 2020.
12. Joshua Rovner, 2020, "What is an Intelligence Contest?" in: *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, Austin: Texas National Security Review. <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>.
13. Ibid.
14. Ibid.
15. Michael Warner, 2020, "The Character of Cyber Conflict" in *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, Austin: *Texas National Security Review*, <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>,
16. Ibid.
17. Jon R. Lindsay, 2020, "Military Organisations, Intelligence Operations and Information Technology" in: *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, Austin: *Texas National Security Review*, <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>.
18. Ken Booth and Nicholas J. Wheeler, 2018, "Uncertainty," in Paul D. Williams and Matt McDonald (eds.), *Security Studies: An Introduction 3rd Edition*, Abingdon, UK: Routledge, 132.
19. Michael A. Jensen and Colin Elman, 2018, "Realisms," In Paul D. Williams and Matt McDonald (eds.), *Security Studies: An Introduction 3rd Edition*. Abingdon: Routledge, 23
20. Charles L. Glaser, 2013, "Realism," In *Contemporary Security Studies* (3rd Edition), edited by Alan Collins, 13-27, Oxford: Oxford University Press, 16.
21. Booth and Wheeler 2018, 133.
22. Ben Buchanan, 2016, *The Cybersecurity Dilemma: Hacking Trust and Fear between Nations*. London: Hurst and Company.
23. Ibid., 23.
24. Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, 2018, *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford: Oxford University Press.
25. Martin C. Libicki, 2012, *Crisis and Escalation in Cyberspace*, Santa Monica: RAND Corporation, xvi.

**NOTES**

26. Martin C. Libicki and Olesya Tkacheva, 2020, “Cyberspace Escalation: Ladders or Lattices?” In A. Ertan, K. Floyd, P. Pernik, and T. Stevens (eds.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn, Estonia: NATO CCD COE, 62.
27. CIVIC, 2021, *Entering the Grey Zone: Hybrid Warfare and the Protection of Civilians in Ukraine*, <https://civiliansinconflict.org/publications/policy/entering-the-grey-zone/>, 17.
28. Adam Meyers, 2016, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units*, CrowdStrike Blog, <https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/>.
29. UN GGE, 2021, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>, 14.
30. ICRC, 2021, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflict*, Geneva: ICRC, 14.
31. Michael Schmitt, 2021, *The Sixth United Nations GGE and International Law in Cyberspace*, Just Security Blog, <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>.
32. ICRC 2021, 15.
33. Paul M. Nakson and Michael Sulmeyer, 2020, “How to Compete in Cyberspace: Cyber Command’s New Approach,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>.
34. Robert Chesney, 2018, *Offensive Cyber Operations and the Interagency Process: What’s at Stake with the New Trump Policy*, Lawfare Blog, <https://www.lawfareblog.com/offensive-cyber-operations-and-interagency-process-whats-stake-new-trump-policy>.



# Three Conditions for Cyber Countermeasures

*Opportunities  
and Challenges  
of Active-Defense  
Operations*

---

Dr. Nori Katagiri

## **ABSTRACT**

*This article explores a variety of opportunities and challenges with the use of cyberspace countermeasures. It critically assesses a set of conditions under which countermeasures can be an appropriate means of offensive cyber: limited aim of defense and deterrence, protection of critical infrastructure, and compliance with rules of behavior. Here, the article shows that countermeasures must be taken for the purpose of active defense and deterrence. Second, they can be appropriate as a means of defending critical infrastructure. Finally, they should be executed by state actors who comply with existing principles of cyberspace behavior. While cyberspace countermeasures can become a socially accepted, legitimate means of active defense and deterrence, the article shows that there are several challenges connected with each of these conditions. For one, there are various degrees of feasibility about what conditions are appropriate for countermeasures. The article also discusses inherent problems in the application of international law, from which rules of engagement are drawn, to cyberspace. The challenges are hard to solve, which may explain why it has been so difficult for the international community to produce a set of agreeable criteria for active defense measures.*

© 2022 Dr. Nori Katagiri



**Nori Katagiri** is associate professor of political science and coordinator of international studies at Saint Louis University. He is the author of *Adapting to Win: How Insurgents Fight and Defeat Foreign States in War*, published by the University of Pennsylvania Press. His works on cybersecurity have appeared in the *Journal of Cybersecurity*, *Global Studies Quarterly*, and *Asian Security*, among other venues. He is a senior fellow at the Irregular Warfare Initiative of the Modern War Institute, United States Military Academy at West Point. Before joining Saint Louis University, he was associate professor of international security studies at the Air War College, a graduate military school of the United States Air Force. He received his Ph.D. in political science from the University of Pennsylvania and served as visiting fellow at the Modern War Institute at West Point, Japan's Air Staff College, Taiwan's National Defense University, and the University of the Philippines – Diliman.

## INTRODUCTION

In recent years, experts have paid growing attention to the need to develop a whole new range of countermeasure options to deter hostile acts in cyberspace. This is a healthy development, as well as a reflection of hackers' increasing capabilities and frequency of attacks. As such, the call for an enhancement of defensive measures to counter the trend is long overdue. Yet it is not entirely clear what makes countermeasures appropriate in cyber operations from the standpoint of legal, ethical, society, and strategic effect standpoints. This article will address the three conditions that need to be met for countermeasures to be an appropriate means of cyber operations and explore both the opportunities and challenges of countermeasures. This article places greater emphasis on the strategic and political aspects of conducting countermeasures in cyberspace than other dimensions, such as legal.

First, countermeasures must be planned and carried out for the purpose of active defense and deterrence. Second, they can be appropriate to defend critical infrastructure. Finally, they should be executed by state actors who comply with existing principles of cyberspace behavior. The second part of this argument is that there are various degrees of feasibility with each of the three conditions. The first two conditions are more practical than reliance on norm compliance. It is also important to note that, while the three conditions do not necessarily represent an exhaustive list of opportunities, challenges, and limitations, they serve as a set of necessary factors for the option of countermeasures to be socially accepted and effectively executed. However, because the conditions are not something that can be easily met, not every country will be able to meet the criteria.

### *The scope of analysis*

In cyberspace, countermeasures consist of several types of measures, including “honeypot” (trapping

attackers for forensic analysis), “dye-packs” (tracing seekers of decoy files), and “hacking back” to neutralize stolen data and disable launch servers. The definition allows us to treat countermeasures as a strategic option whose use would be consistent with some of the most important principles of cyberspace behavior, including proportionality and compliance with international law. However, it does not allow us to differentiate countermeasures from other forms of cyber operations. For instance, how are our countermeasures distinguished from offensive cyber operations (OCO), defined here as “missions intended to project power in and through cyberspace”?<sup>[1]</sup> How do we know which comes first: enemy attacks (“another State’s unlawful action”) and countermeasures when enemy attacks are frequent and inconsistently responded to? How can we explain the timing and sequence of actions? Public discourse continues to progress under the assumption that answers to these questions would eventually be found.

In this article, countermeasures are defined as a set of responses toward verified attackers within a reasonably short period of time. Countermeasures differ clearly from unprovoked attack operations because they are a response to strikes launched unjustifiably. Instead, countermeasures are a subset of active defense activities, which include a wider set of actions like indictments and sanctions against attackers.<sup>[2]</sup> Active defense is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of such threats. It differs from passive defense, which involves a wide range of key tasks to reject incoming attacks through security patches, backups, warning systems, and education.<sup>[3]</sup> The differences are subtle, however, between countermeasures because these actions often occur simultaneously. In fact, except for the unprovoked offensive missions, the defensive measures are in a relationship of mutual reinforcement. Countermeasures are part of key discussions on some of the most recent policies to deal with cyberspace vulnerability. Conceptually, countermeasures are utilized as part of the existing cyber toolkits under the US policy of persistent engagement and defend forward, where the US would closely observe the planning of adversaries and inform partners to take action themselves.<sup>[4]</sup> Although not explicitly stated, countermeasures can be conducted as an active defense component within a broader cyber defense framework; persistent engagement is partly designed to counter adversaries’ measures to attack US infrastructure as a means to help develop their own countermeasures.<sup>[5]</sup>

Technologically capable states have developed expertise within their bureaucracies and worked with the private sector to devise plans to develop options individually. Collective countermeasures give additional options to countries with similar threat perceptions, although those are mostly already in formal alliances.<sup>[6]</sup> For instance, within NATO, experts have worked on collective options for some time, a development that may encourage allies elsewhere to consider similar options.<sup>[7]</sup> However, a horizontal spread of collective countermeasures would take time because in reality, few cyber-active states are in such a privileged position as NATO. Many US defense-treaty allies in the Indo-Pacific, such as Japan and the Philippines, have not yet entered

serious discussions about building a joint architecture, largely because their networks are less integrated and because their alliances with the US are bilateral, rather than multilateral.<sup>[8]</sup> Even within NATO, there have been calls for restraint against the immediate adaption of its collective defense clause to cyberspace. This is because, according to Jeppe Jacobsen, to do so would risk “undermining the cyber-intelligence norm that so far has prevented escalation and thereby increasing the likelihood that Russia misinterprets intelligence and active cyber defense activities as military preparation, armament or an attack in the making.”<sup>[9]</sup> This discussion underscores the existence of various degrees of acceptability of collective countermeasures.

It is also important to note that while the private sector, especially technology and consulting industries, plays an integral part of countermeasure research and development, only states, and collective defense mechanisms like NATO, would let private actors be justifiably involved in *defensive* measures but not deploy offensive measures.<sup>[10]</sup> This is due to the fundamental difference between private and public sectors about their basic functionality. Private businesses operate according to financial logic, while governments have national security responsibilities and are under constant scrutiny on how they execute these responsibilities. As a result, most states refrain from engaging private companies directly in attacking foreign servers.<sup>[11]</sup>

The literature on cyber countermeasures is expanding, with political scientists exploring the functionality of measures like hacking back as a set response to security incidents.<sup>[12]</sup> Many in private business have explored offensive cyber techniques for financial gains and investment opportunities.<sup>[13]</sup> Policymakers have increasingly accepted countermeasures as a topic of consideration, possibly more so than the concept of offensive cyber itself. Yet the cyber community has not figured out how to conduct offensive cyber responsibly while minimizing the negative consequences it may cause, such as escalation of tension.<sup>[14]</sup> There are technical challenges that need to be addressed, too, including how to design and oversee operations and test tools before launching while preventing criminal and third-party access to backdoors.<sup>[15]</sup> There are three important conditions that should be met as we move forward with the discussion on countermeasures in the framework of offensive cyber.

### ***1. Limited aim of defense and deterrence***

The first condition for countermeasures is that they be used not for the purpose of preemption but for defense and deterrence through retaliation and punishment. Countermeasures are most permissible when launched as an act of denying and dissuading future attacks by threatening to impose costs on attackers. The active-defense use of countermeasures is meant to mitigate the persistent failure of the current preventive mechanism to discourage the global proliferation of hostile cyber operations. The spread of malware has accelerated to such a great degree as more malicious actors develop offensive capabilities and gain access to various hacking tools.<sup>[16]</sup> Countermeasures should then impose reasonable amounts of pain to deter potential attackers. At the same time, countermeasures must be clearly delineated from unprovoked OCO, defined above.

As such, restraint is a critical condition for countermeasures. To make them solely used for the purpose of defense and deterrence, however, actors must meet several sub-conditions. First, countermeasures must be declared publicly, rather than threatened opaquely. Policymakers need to clarify conditions under which they would act defensively and carry through the process to keep their actions credible. When properly executed, declaratory countermeasures allow policymakers to avoid so-called “gray zone” situations and keep attackers from abusing the opaqueness to their advantage by way of plausible deniability.

Second, policymakers need to know that cyber defense and deterrence is hard, with the latter likely harder. Defense and deterrence, respectively, call for different requirements. On the one hand, countermeasures for defensive purposes presume that policymakers, presumably through expert intermediaries, (1) know of the existing vulnerabilities in their systems; (2) can detect an attack and attribute reasonably quickly; (3) know that defense without countermeasures would be insufficient because defense alone has no “teeth.” These criteria are already challenging for technical, legal, and political reasons.<sup>[17]</sup> Only a small number of states have the technological prowess to launch countermeasures in this situation. On the other hand, it is extremely difficult to draw clear effects from countermeasures launched for *deterrence*. Deterrence is invisible; we do not see a thing move when deterrence works. In effect, when a cyber-attack is thwarted, we are tempted to assume that deterrence is not responsible for the lack of action. This is especially tempting because most states accused of perpetrating cyber operations typically do not confirm or deny responsibility.<sup>[18]</sup> Michael Fischerkeller and Richard Harknett contend that “the protection ... of national interests cannot rest on deterrence as the central strategy” and call for the use of active cyber operations to shape normative expectations of behavior.<sup>[19]</sup> Views like this have emerged in government policies. For example, Britain’s National Cyber Strategy of 2020 posits that its “approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers.”<sup>[20]</sup>

Another challenge stems from the inherent difficulties in defense and deterrence that render countermeasures an inadequate form of response. In other words, had defense and deterrence been adequate, countermeasures would not be needed. This argument has some merits; after all, the addition of countermeasures to defenders’ toolkit is likely to broaden the mission to the extent that it becomes hard to keep the aim “limited.” The concern with mission creep can be mitigated, however, when actors declare intent on countering in advance and if they launch countermeasures clearly and demonstrably for defensive purposes. When states make clear their conditions for launching countermeasures, they simultaneously reduce the chance of escalation.

## ***2. Defending critical infrastructure and its challenges***

Countermeasures are appropriate when deployed to defend critical infrastructure from cyber-attacks. In the face of the recent rise of ransomware attacks and public attention on the need to defend critical infrastructure, the public is more readily accepting of countermeasures.

As resources are limited, decision makers must prioritize which sectors of the network to defend. However, as of June 2022, while there are many national guidelines and policies on critical infrastructure, there are no global guidelines on what critical infrastructure is and how we can digitally protect it, which then allows states to operate with various sets of definitions.<sup>[21]</sup> When the US identifies a set of 16 sectors, Russia’s “critically important objects” are six, with 48 different sub-sectors.<sup>[22]</sup> There are countries without a definition, including China. Beijing refers to critical information infrastructure (CII) as systems that, “if destroyed, suffering a loss of function, or experiencing leakage of data might seriously endanger national security, national welfare, the people’s livelihood, or the public interest,” but there are no components given as examples.<sup>[23]</sup> This means that every conceivable item can be considered an illegitimate target in China’s cyberspace, so any cyber-attack on China could be interpreted as one on CII, a ground for retaliation. That is why, for instance, RAND researchers fear that “cyber activity on the power grid that fits well within one country’s definition of espionage could be interpreted by another country as an imminent attack.”<sup>[24]</sup>

The problem is that hackers may not be on the same page as to what states consider critical infrastructure. They may not have a clear idea of what critical infrastructure includes and what is considered an illegitimate target. Besides, if critical infrastructure crosses so many properties at once, how are hackers supposed to know what to avoid *and* how to avoid them in their operations? Are there any targets that can be “legitimate”? The questions are critical because there is no communication between hackers and states about what they mean “legitimate” targeting is, if any. This lack of mutual understanding allows hackers to invoke plausible deniability and unilaterally expect victims to take no preventive action, another recipe for disaster.

Not surprisingly, this problem is not limited to critical infrastructure; research points to similar problems in supply-chains sectors. A study of government policy in Britain, the US, and the European Union on chemical, energy, and water sectors unearthed a variety of interpretations for “supply chain,” which resulted in different quantities and qualities of advice offered by authorities and sectors. The absence of a common language has generated challenges to support supply chain procurement, risk management, and limited coverage.<sup>[25]</sup> Solutions to these challenges are hard to come by, in part because they need to come not from individual states but from the international community at large. While the international community would need to determine what sectors would be protected and ensure that hackers know it, achieving this is difficult as sectors that would be excluded from the category would certainly oppose this effort. Debate would take years to complete, if at all, requiring stakeholders to determine which sector would be considered as critical infrastructure. To coordinate in the prototypical “two-level negotiation” is extremely hard, especially because countries have conflicting priorities and different amounts of resources to spend on it.

### ***3. Compliance with rules of behavior***

Finally, countermeasures are legitimate when they conform to a host of behavioral norms. This condition has been debated for over a decade in venues like the United Nations (UN) Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG). Making sure that cyberspace activities comply with existing global rules ensures the legitimacy of its operations. Another reason why we need explicit signs of international compliance is that some states would otherwise consider countermeasures excessively provocative. They may find it so controversial to carry out countermeasures that they require international approval before going ahead with them. Countries like Japan, for instance, have tried to move forward to strengthen their defenses through cross-domain concepts, but Japan has found it quite difficult to carry out active defense because of its unique constitutional, social, and political environments.<sup>[26]</sup> National debate has proceeded to where officials have refrained from officially developing cyberweapons for defense. Thus, for countries to move forward with the agenda of countermeasures, they must first make efforts to craft a strategic framework in which countermeasures would gain public legitimacy through voluntary compliance with rules of behavior.

The importance of adherence to cyberspace norms has been widely recognized in cybersecurity literature. Strategic cyber scholars have stressed the role of ethical integrity as a key enabler of norm diffusion,<sup>[27]</sup> but they also emphasize the social benefits of operational restraint.<sup>[28]</sup> Furthermore, they stress the need for us to understand how international rules encourage actors to comply with norms of cyberspace behavior and to merge humanitarian values with technical expertise.<sup>[29]</sup> The call for synergy has prompted the participation of major technology firms like Microsoft in the discourse around setting norms and increased the number of advocates for a ban on attacks on critical infrastructure.<sup>[30]</sup> For example, Robert Collett stresses communication and consultation to generate an actionable framework, prioritize national capacity needs, and give compelling narrative to consolidate the outcome.<sup>[31]</sup>

Under the principles of necessity and distinction, respectively, states would launch countermeasures only when they faced grave and imminent peril and would do so in ways that avoid causing excessive harm or hitting civilians and units used by noncombatants for nonmilitary purposes (for instance, hospitals). Under the principle of proportionality, states would not launch countermeasures in ways that would be excessive relative to the strike against them. Under the principle of due diligence, states should be proactive so that their territory is not used for operations that produce adverse consequences for other states.

Even though each of these principles works differently, they remain mutually beneficial. That is, the more principles are respected by the international community, the more likely they are to have collective effects against illicit actions. Furthermore, the more states complying with each of the principles, the more likely the international community is to have stronger legitimacy in using the principles to discourage malicious operations. Yet the interlocking

relationship of the principles and actors presumes that there must be a critical mass of countries that abide by the principles. The challenge is that there is a limited number of states able and willing to comply with the principles.

At the same time, policymakers must acknowledge that these principles will not be a perfect shield against malicious actions. Research shows that they are especially ineffective against OCO by non-state actors.<sup>[32]</sup> Partly because of these problems, the norms and principles stated above have repeatedly been ignored. Hackers have collaborated with China, Russia, North Korea, Britain, and the US to spy on each other to help them reinforce their great power ambitions.<sup>[33]</sup> The GGE and OEWG are gathering to address a range of enforceable conditions under which violators of the laws and norms would be penalized.

### CONCLUSION

In this article, I discussed some of the most important strategic aspects of conducting countermeasures as part of offensive cyber. Countermeasures can be justified as an appropriate mode of offensive cyber under the assumptions of the limited aim of defense and deterrence, protection of critical infrastructure, and compliance with rules of behavior. At the same time, there are challenges with carrying them out as a form of offensive cyber. First is that there are various degrees of feasibility about what conditions can be met for countermeasures to be appropriate. Second, there are challenges with meeting each of the conditions themselves. The challenges are hard to solve, which may explain why it has been so hard for the international community to yield a set of agreeable criteria for active defense measures. It is also important to note that strategic effectiveness and legality may not necessarily equal ethical maturity of options even if they are conducted for purely defensive or deterrent purposes, because they involve intrusive actions that can be seen as “offensive.” This suggests that there may be other conditions we may have to examine.

All this leads to a somewhat pessimistic assessment of countermeasures as part of offensive cyber. There is no excuse, however, for the international community to not develop more defensive and deterrent options. The aim of this paper was to describe opportunities for active defense options, spell out relevant challenges with the process of carrying out the measures, and generate a host of solutions to deal with them. More work need to be done, especially in terms of finding out what other components of countermeasures need to be put into a comprehensive framework of offensive cyber to make them a legitimate means of active defense.📍

## NOTES

1. The US Department of Defense, *Cyber Operations, Joint Publication 3-12* (June 8, 2018).
2. Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman & Littlefield: Lanham, MD, 2017), 18-9.
3. Dorothy Denning and Bradley Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," in *Understanding Cyber Conflict: 14 Analogies*, eds. George Perkovich and Ariel Levite (Washington, DC: Georgetown University Press, 2017), 194.
4. Fifth Domain, "Here's how Cyber Command is using 'defend forward'" (November 12, 2019).
5. Michael Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review*, Special Edition (2019), 276-77.
6. See NATO, "Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations" (January 2020), 22.
7. See, for instance, Chon Abraham and Sally Daultrey, "Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK," NATO CCDCOE, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (Tallinn, Estonia, 2021).
8. It is possible that the recent development of the trilateral security pact between Australia, the United Kingdom, and the United States (AUKUS) may bring Australia even closer to the ties between Britain and the United States. On the other hand, US allies like Japan may be tempted to be part of growing collaboration among these countries, especially through the ongoing Quad cooperation mechanism (Australia, Japan, India, and the United States), although as of June 2022, Japan's case is restricted to its bilateral alliance with the United States. The Guardian, "Japan should work with Aukus on cyber-security and AI, says Shinzo Abe" (November 19, 2021).
9. Jeppe Jacobsen, "Cyber offense in NATO: challenges and opportunities," *International Affairs*, Vol. 97, No. 3 (May 2021), abstract.
10. James Pattison, "From defense to offence: The ethics of private cybersecurity," *European Journal of International Security*, Vol. 5, No. 2 (2020), 233-34.
11. Michael Chertoff, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (New York: Grove Press, 2018), 188-91.
12. Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press, 2020), 113-200.
13. Cyberscoop, "A 'lot' of firms are developing offensive cyber techniques, hoping for investment" (October 18, 2021).
14. Lawrence Cavaola, David Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival*, Vol. 57, No. 1 (2015); Jason Healey, "The Cartwright Conjecture: The Deterrent Value and Escalatory Risks of Fearsome Cyber Capabilities," in Lin and Zegart, eds., *Bytes, Bombs, and Spies*.
15. Perri Adams, Dave Aitel, George Perkovich, and JD Work, "Responsible Cyber Offense," *Lawfare* (August 2, 2021).
16. Cyberscoop, "Nations investing in cyber, 'democratization' of malware are factors accelerating dangers online, CISA official says" (October 18, 2021).
17. Paul Ducheine and Peter Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in Frans Osinga and Tim Sweijs, eds., *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice* (The Hague: T.M.C. Asser Press, 2021), 487.
18. Joseph Brown and Tanisha Fazal, "#SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations," *European Journal of International Security*, Vol. 6, No. 4 (2021).
19. Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis*, Vol. 61, No. 3 (2017), 382.
20. The Cabinet Office of the United Kingdom, *National Cyber Strategy* (2022), 25.
21. Cecilia Gallais and Eric Filiol, "Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure," *Journal of Information Warfare*, Vol. 16, No. 1 (Winter 2017), 64-65.
22. Christer Pursiainen, "Russia's Critical Infrastructure Policy: What do we Know About it?" *European Journal for Security Research*, Vol. 6 (2021), 25.
23. Graham Webster, Samm Sacks, and Paul Triolo, "Three Chinese Digital Economy Policies at Stake in the U.S.-China Talks," *New America* (April 2, 2019).

**NOTES**

24. Anu Narayanan, et al., *Detering Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense* (Santa Monica, CA: RAND Corporation, 2020), pp., xv-xvi. Also see Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford: Oxford University Press, 2016), Chapter 4.
25. Colin Topping, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid, “Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks,” *Computers & Security*, Vol. 108 (September 2021).
26. Nori Katagiri, “From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations?” *Asian Security*, Vol. 17, No. 3 (2021).
27. Martha Finnemore and Duncan Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal of International Law*, Vol. 110 (2019).
28. Joseph Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3 (Winter 2016/17), 60.
29. Matthias Kettemann, *The Normative Order of the Internet: A Theory of Rule and Regulation Online* (Oxford: Oxford University Press, 2020).
30. Louise Marie Hurel and Luisa Cruz Lobato, “Unpacking cyber norms: private companies as norm entrepreneurs,” *Journal of Cyber Policy*, Vol. 3, No. 1 (2018).
31. Robert Collett, “Understanding cybersecurity capacity building and its relationship to norms and confidence building measures,” *Journal of Cyber Policy* (2021).
32. Nori Katagiri, “Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks,” *Journal of Cybersecurity*, Vol. 7, No. 1 (2021).
33. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020).





# The Failure of Offense/Defense Balance in Cyber Security

---

Dr. Brandon Valeriano

## ABSTRACT

*The idea of offensive advantage dominates the cyber security field, a framework originating from research on the offense/defense balance in conventional warfare. The basic theory is that the balance of offensive and defensive forces determines what kind of strategy will be most effective. The field of cyber security consistently tries to build on offense/defense balance frameworks with little awareness of the inherent problems of the theory. If the offense is dominant, then the defense would supposedly never win against an aggressive adversary due to the compounding nature of failure. The only solution would be going on the offensive in return. This article identifies three core problems with applying the offensive/defensive balance to cyberspace: (1) the inability to distinguish between the two frames, (2) the failure to understand the impact of perceptions, and (3) the inaccuracy of measurement. The pathology of offensive advantage and being under siege as a defender can only continue to lead to strategic malaise and constant attacks as the defender fails to shore up vulnerabilities due to the mistaken belief in the ascendancy of the offense.*

## DOES THE CYBER OFFENSE HAVE THE ADVANTAGE?

There is a simple conjecture that is quite common in all aspects of society: the best defense is a good offense. The idea, offered by no less a luminary than George Washington in a letter to John Trumbull, shapes how many think about engaging any adversary. Washington wrote, “It is unfortunate when men cannot, or will not, see danger at a distance [France]...not less difficult is it to make them believe, that offensive

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



**Brandon Valeriano** is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University and served as senior advisor for the Cyberspace Solarium Commission. Valeriano has published six books and dozens of articles for such outlets as the *Journal of Politics*, *International Studies Quarterly*, and the *Journal of Peace Research*. His two most recent books are *Cyber War versus Cyber Reality* (2015) and *Cyber Strategy* (2018), both with Oxford University Press. Valeriano has written opinion and popular media pieces for such outlets as the *The Washington Post*, *Slate*, *Foreign Affairs*, and *Lawfare*. His ongoing research explores conflict escalation, big data in cybersecurity, the cyber behavior of revisionist actors, and repression in cyberspace. Valeriano has a PhD from Vanderbilt University. drbvaler@gmail.com

operations, often times, is the surest, if not the only (in some cases) means of defense.”<sup>[1]</sup>

The basic premise of the idea is historically and theoretically wrong. The US would clearly not have benefited from an offensive war against France in 1799 when the new nation were barely able to handle the Barbary pirate nations a few years later. The perceived utility of the offense persists and promotes the belief that action can trump protection in cyber security because of its simplicity and the general failure in the field to evaluate claims with evidence. Avoiding prudence and restraint in favor of offensive superiority is a notion that continues to pollute the discourse.

The ideal of offensive advantage dominates the cybersecurity field, carried over from research on the offense/defense balance (hereafter the O/D balance) in warfare.<sup>[2]</sup> The basic framework offered by Lynn-Jones is that “there is an offense-defense balance that determines the relative efficacy of offensive and defensive security strategies.”<sup>[3]</sup> Ever since visions of *Wargames* (1982) and thermonuclear war launched by out-of-control computers entered the imagination, conventional wisdom quickly called for offensive action against emergent technological threats.

For some, technology and computers are so vague and unknown that what becomes conventional wisdom often lacks basic logic. Strategists believe cybersecurity is offense-dominant, attacking first and sorting out the damage later becomes the guiding star for cyber strategy. Understanding exactly what the cyber offense is would be helpful; the basics would be a focus on attack and maneuver. There is an idea of going forward and operating outside of one’s networks to deny options to the adversary. The defense is simple to explain in this context. It is about protections and ensuring the homeland infrastructure is secure to prevent the worse abuses of cyberspace.

The benefit of prioritizing offense in cyber operations is a critical question. Belief in the utility of aggression is dangerous; it is also likely a reaction to the threat inflation pervasive in the discourse. Employees of the US government are fond of saying that they are taking fire from all sides in cyber operations. This pathology of offensive advantage and being under siege as a defender, reinforced by patterns promoted by the media and the Twitter discourse of constant cyber barrage, can only continue to lead to strategic malaise and constant attacks as the defender fails to shore up vulnerabilities due to the mistaken belief in the ascendancy of the offense.

In this article, I review the foundations of the dominant idea of cybersecurity offense being the best defense. I demonstrate the flawed logic of this framework and push for ideas that break the limits of it. Why does the community waste its time with a research program the security studies field already discarded?

## FAILURE OF AN IDEA: THE OFFENSE/DEFENSE BALANCE

### *Origins and Failure of an Idea*

The basic premise of the O/D balance is that “when defense has the advantage over offense major war can be avoided.” This simple conjecture has created a field of research that seeks to unlock the mysteries behind war and peace by focusing on the nature of operations and perceptions of advantage.<sup>[4]</sup> That so many gravitate to the O/D balance in cyberspace demonstrates a failure to understand the history of the discipline and the lessons learned by those who came before. While research on the O/D balance exploded in the 1980s and 1990s, mainly due to early work by Snyder and Van Evera, it was on life support by the time Van Evera’s book *Causes of War* appeared in 1999.<sup>[5]</sup> Proposing a solution to the problem of war and peace, instead the literature became confused over how to measure the phenomenon and even what the central variables were. Van Evera (1999) laid out five hypotheses ranging from false optimism for creating the conditions for war to war being likely when conquest is easy. The paradigm stuttered and moved toward different versions of realism that were more parsimonious and not based on subjective perceptions of offensive power.

A theorist's belief that offense is best is, at best, an outcome after the fact and, at worst, an outcome dependent on rational perceptions of the O/D balance. The ideal of the O/D balance, even if accepted that it is empirically accurate and measurable, is both doubtful and fails to motivate action clearly. States assuming a systemic offensive advantage might be deluded in their perspective, as happened during World War I, or they will go on the offense anyway due to the power of other motivating variables, such as a desire for a territorial claim.<sup>[6]</sup>

Levy notes that “the concept of the offense/defense balance is too vague and encompassing to be useful for theoretical analysis.”<sup>[7]</sup> Three core problems emerged on top of the issue of uncontrollable outcomes not being impacted by post hoc reasoning. The first is that offense and defense are indistinguishable, or at least an observer cannot tell which is which. The second problem is that the foundation of theory is based on the rational perception that there must

be an advantage to offense or defense, either dyadically or systemically. This is based on the premise that leaders will make optimal choices. The final issue is how to measure the factor of offense/defense empirically.

### *The Cyber Balance*

A misguided focus on the balance between offensive and defensive operations clouds understandings of cyber strategy and forces practitioners toward language that does not describe the nature of cyber operations. It is nearly impossible to distinguish cyber actions between offense and defense and even more so difficult to measure said actions. To assume that the balance between offense and defense can be accurately measured and perceived by leaders requires the theorists to comport themselves into so many leaps of logic that the mental gymnastics become impossible.

The developing field of cybersecurity quickly gravitated toward examining the O/D balance in cyber interactions due to the simplicity of the framework. For Healey (2021), it is not important to understand who has the advantage, but under what conditions the framework operates. Such a view presumes that there is an advantage in the first place and that perceptions of the adversary can be known.

The field of cyber conflict continues to build on early ideas by some such as Buchanan (2016), who noted that the offense is ascendant over the defense. Fischerkeller and Harknett have advocated for the strategic doctrine of cyber persistence because the enemy is persistent and the only way to counteract an adversary's offensive cyber actions is to take even earlier offensive action.<sup>[8]</sup> Healey notes, "Since the beginnings of the internet, the offense often has *seemed to* have the advantage over the defense."<sup>[9]</sup>

Unfortunately, there is no evidence that the offense has an advantage or that it is the best course of action in cybersecurity. Some arguments for offense dominance are based on the ubiquity of certain systems and companies, like Microsoft.<sup>[10]</sup> Since the Internet was never built for security in the first place, it stands to reason that it must then be largely insecure. Healey notes that defensive failures cascade and proper targeting can lead to offensive advantages.<sup>[11]</sup> The defense supposedly can never win against such adversaries due to their power and reach, the compounding nature of failure, and the specific difficulty of protecting all systems from known and unknown vulnerabilities.

The marketplace of ideas does provide alternative frameworks. Early research on all known cyber interactions demonstrates restraint rather than uncontrollable aggression in cyberspace.<sup>[12]</sup> In fact, escalation is rare<sup>[13]</sup> and retaliation nearly non-existent.<sup>[14]</sup> Early on, Gartzke and Lindsay noted the importance of deception in cyber operations, a form of defense mostly.<sup>[15]</sup> Slayton notes that the balance between defense and offense is conditional on organizational processes and the cost of the bureaucracy, not the raw impulses of the aggressive actor.<sup>[16]</sup> The remainder of this article examines three core flaws in theory of the O/D balance as it relates to cybersecurity.

## **DISTINGUISHING INDISTINGUISHABILITY**

The key challenge for the issue of an offense/defense balance, or even simple discussions of the offense or defense in cyberspace, is that it is nearly impossible to distinguish between the two. How do you tell which is which? The fluidity of the concept of offense or defense makes the terms virtually useless, since it is near impossible to operationalize, the terms making the research imprecise. Moves that are said to be defensive involve forward maneuver that can seem offensive in nature. Offensive operations set to impose costs on the opposition are often thought to be defensive in nature, for example, indictments or sanctions against digital aggressors.

Terms on shaky definitional grounding are prone to conceptual stretching. The term “conceptual stretching” was originally coined by Sartori, who connected the idea to the distortion that comes when a concept does not fit new cases.<sup>[17]</sup> This factor is at play often in cybersecurity where new cases confound observers. Does the US rerouting of server traffic for a ransomware group count as an offensive or defensive operation?<sup>[18]</sup> Certainly, the operation is proactive and involves foreign network space, but the operation is also not destructive or violent and represents a move to protect the American homeland from ransomware attacks on civilian targets that seemingly plagued the US during the pandemic.

Ideas that defy basic categorization are prone to confirmation bias and the assumption that the measurement is correct when the term itself defies basic measurement. The “offense” and “defense” are terms that are difficult to operationalize. What exactly is an offensive and defensive operation in cyberspace? The problem is any desire to operationalize a difference between offensive and defensive operations is based on an artificial division of the problem. It is not a problem of being precise, but rather distinction. Much like the Dutch ideal of “total football,” the best defenders are also the best attackers.<sup>[19]</sup> They know the weak spots and where to look for vulnerabilities; just as the best attackers are also the best defenders since they know the attack surface so well and can pinpoint weaknesses. The strategic logic between the distinction is empty, yet there is a logic to force allocation and structure that might require a division between defensive and offensive forces, a distinction that remains artificial.

Cyber confusion pervades discussions of the offense and defense. Is a zero-day vulnerability (an unknown flaw) an offensive weapon? Some might suggest any unknown vulnerability can be exploited by the attacker. Yet it is just as likely that basic probes or vulnerability research on other targets will uncover the unknown vulnerability, and allow the defender to become stronger once the weakness is patched. An unknown vulnerability can be both defensive and offensive at the same time, making the idea of distinguishing between the two frames nearly impossible.

What of national cyber forces such as the Cyber Mission Force in the U.S. Cyber Command (USCYBERCOM) or the National Cyber Force in the UK? While these forces can go on the

attack against other nation-states, they also can be posted as defensive operators seeking to stop attacks before they happen. The reality is that the active and adaptive nature of modern technology makes the idea of distinction between offense and defense entirely empty, resulting in the basic research question being almost meaningless.

## PERCEPTIONS

A key foundation of the offense/defense balance is that perceptions will be optimal. One side will perceive either the offense or defense as having the advantage determining the probability for war. Yet, as critics have pointed out, “It is inherently difficult to assess the impact of weapons technologies, particularly when they have not been employed in war.”<sup>[20]</sup>

Glaser and Kaufmann note that versions of realism need to introduce a variable that converts power into military capabilities for the theory to be operational.<sup>[21]</sup> This becomes a key condition to provide a mechanism for how the process of an O/D balance must work to influence the dependent variable, taking territory or winning wars. The remaining question is whether the perceptions of how technology creates military capability accurate?<sup>[22]</sup> How does a state decide if one is operating in an offensive- or defensive-dominant situation?

Views of cyber power and an emphasis on offensive dominance are really in the eye of the beholder. There is no standardized method of measuring cyber power. In a 2018 book, Valeriano et al. developed a measure of latent cyber capacity measuring digital infrastructure and knowledge capital (engineering graduates and patents).<sup>[23]</sup> South Korea came out ahead of the US, China, Japan, and Israel, in that order. Clarke and Knake list a ranking of the US, Russia, China, Iran, and North Korea.<sup>[24]</sup> The Belfer Center National Cyber Power Index of 2020 ranks the US, China, and the UK (a new entry) as the top-three due to the inclusion of a variable for intent, which is coded subjectively based on readings of documents.<sup>[25]</sup>

For cyber security, converting cyber power into military capabilities is a fraught enterprise. There is little evidence that cyber power is coercive, on either the diplomatic or military battlefield. Kostyuk and Zhukov note there is no impact from cyber capabilities on the battlefield in Ukraine, a finding which appears to be holding strongly during the Ukraine War that began in 2022.<sup>[26]</sup> In a macro study, Valeriano et al. find little evidence of a coercive impact on international relations, with most cyber events failing to change the behavior of the target.<sup>[27]</sup> When the target’s behavior changes, it is often as a defensive maneuver to prevent future incursions. If the central mechanism of the O/D balance is the fact of coercive change through technology, cyber options play little role in this process.

The problem is that, for some, cybersecurity is revolutionary, yet there is no evidence that cyber operations affect the battlefield.<sup>[28]</sup> There are assumptions of a Battlestar Galactica (2004) effect in which the opposition shuts down all weapons and communications making the target’s defenses inoperable to the point of fantasy. This perception of effectiveness, disconnected from the empirical reality of the impact on operations, demonstrates the pervasive power and

inapplicability of O/D balance theory to cyberspace. In a domain that operates mostly without empirical evidence, anyone can perceive whatever he/she chooses, often based on fictions, yet the reality is often much different.

The idea that a state's perception of the O/D balance can be accurately known by the opposition is betrayed by the inability of the aggressor even to understand its operations and to optimize their security. That many misperceived the power of the offense on the eve of World War I should suggest that the theory is on shaky ground from the start.<sup>[29]</sup> Even proponents note "this also means that when states do engage in suboptimal behavior, our ability to determine the offense-defense balance by observing military policies and war outcomes is greatly reduced."<sup>[30]</sup> Lynn-Jones argues that states which fail to accurately assess the arena and "adopt offensive strategies in a world of a defensive advantage will be punished by the system."<sup>[31]</sup>

The history of cyber security is a history of suboptimal security behavior since the domain was never developed with security in mind. Of course the policy failures have been constant.<sup>[32]</sup> Debate over whether the offense or defense has the advantage in cyberspace will never be resolved satisfactorily because security was an afterthought in the creation of the Internet. Hence, one must wonder just how critical the research question is when there are no accurate answers offered.

## MEASUREMENT

The water's end for O/D balance is that it is simply impossible to measure the success or failure of the theory given the conditions laid out by its proponents. As Lynn-Jones notes, "The empirical rejection of the framework, plus the more complicated question of just how to measure what an offensive weapon is versus a defensive weapon, and the examined question of how to measure perceptions of these weapons, makes this framework problematic."<sup>[33]</sup> In examining the efficacy of the theory statistically, Gortzak and Haftel find little empirical support for any of the theoretical propositions.<sup>[34]</sup>

Absent of measurement, scholars and policymakers are making predictions that can never be falsified. In short, we can never know if one is wrong, or right. In their effort to save the theory of O/D balance in light of penetrating criticisms, Glaser and Kaufmann counter the idea that the theory cannot be measured "as simply incorrect."<sup>[35]</sup> They note "that the offensive-defensive balance should be defined as the ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender's forces." A line in the sand clearly drawn by scholars, but this point is also degenerative from the earlier grand positions of the O/D balance as the key factor in explaining war and peace.<sup>[36]</sup>

The reformation of O/D balance as simply the ratio of costs for the attacker versus the costs to defend territory is inoperable for cyber security for one simple reason: there is no territory to take. In its simplest form, cybersecurity is about maintaining networks and protections to ensure that systems operate. One can knock out a system, distract the opponent, or confuse

a target but the opposition will always recover at some point. There is rarely a conception of destruction in cyberspace and, although some materials can be destroyed, they can also be quickly restored.<sup>[37]</sup> While some might use the language of maneuver and gaining ground in cyberspace, there is no ground to take.<sup>[38]</sup>

The challenge of distinction then returns: how would one measure the costs to defend versus the costs to attack? Glaser and Kaufmann dismiss all these challenges to suggest that “ball-park estimates of the balance may be sufficient,” demonstrating how shaky the premise is in operation.<sup>[39]</sup> Healey supports this notion by writing, “Exact measurements may be difficult but fortunately are not needed, as the scale and magnitude of the trends should be enough to determine the relative advantage over time between offense and defense.”<sup>[40]</sup>

While it might be simple to classify the O/D balance in the abstract, would one classify USCYBERCOM as offensive and the Department of Homeland Security (DHS) as defensive? Failures at such simple distinctions reveal the fluidity of computer network operations and the pace at which bureaucratic organizations operate and share talent. There is also the compound issue of how to measure the cost of a bureaucracy. Operation costs vary by year and often fail to factor in the costs of training and education outside the network security realm. In short, time and the nature of organization matter a great deal in cyber security when considering the measurement of the O/D balance.<sup>[41]</sup>

While it is difficult to measure O/D balance in any formation based on a dyadic notion of contestation between two entities, it is even more difficult to measure O/D balance in its wider systemic sense. In short, how to do we classify eras exactly? The issue of perceptions returns. How would one know if a set of years under examination is offensive-dominant, especially in light of any objective means of assessment of cyber security operations?<sup>[42]</sup> Regardless of the academic debates on the nature of the O/D balance, the uncertainty that results from the discussion regarding measurement should give anyone pause in the belief that cyber operations can be classified as offensive or defensive.

## FUTURE TASKS

Questions that lack a theoretical grounding or a method of empirical observation to adjudicate outcomes inevitably lead down degenerative pathways, a problem that often pervades the cybersecurity literature. Assuming that there is a distinction between offense and defense ignores the fact that, in practice, the two are impossible to distinguish. Because there is no distinction between the two in practice means that it is impossible to measure the success or failure, which makes the theory indeterminate. Sometimes one must reject the basic premise of a research question if it does not help one understand an issue or provide solutions.

The lessons extracted from this article are very simple. The stopping point for applying O/D balance theory to cyber operations is that it is impossible to distinguish the attack from the defense in cyber security. Effective operationalization of theory is the key consideration. The

inability to create a definition that clearly categorizes the two supposed sides of military operations suggests the theory is unworkable in cyber security. It is not that cyber security cannot be measured and operationalized, but that doing so must be done carefully and should be scientifically valid.<sup>[43]</sup>

There are times when dividing between the offense and defense does make sense. To properly allocate forces, it sometimes becomes necessary to group forces into offense and defense. It might be critical bureaucratically to distinguish between the two sides of offensive and defensive forces, yet this practice is also artificial and often restrains the career paths of defensive operators.

Conflict is a continuum. States build toward conflict; little actions taken can add up and interact with big factors such as territoriality to produce warfare. Distinguishing between offensive and defensive eras has no impact on these actions that lead to war, but it might be able to highlight when a war might occur. This is an interesting proposition but one that requires an accurate reading of perceptions in the domain and the shape of the balance, a near impossibility in cybersecurity.

The premise of O/D balance theory provides poor policy advice, and sometimes leads policy-makers to propose offensive operations when these operations might be unsuited for the domain or, worse, ineffective. Ignoring efforts to establish resilience is a certain condition toward instability and further conflict. The reality is that O/D balance theory is troubling because it minimizes the need for defense and focuses on the magic bullet of emergent technology. While some might argue that we have failed to establish effective defense for cyber operations, the reality is that states have rarely tried to do the defense correctly due to bureaucratic issues, money, lack of knowledge, or the pull of the offense. The misapplied and dangerous conjecture that the best defense is a good offense must end. The best defense is a real defense.🛡️

**NOTES**

1. G. Washington, 1799, From George Washington to John Trumbul, June 25, 1799, J. Trumbul, Mount Vernon.
2. J.S. Levy, 1984, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28(2): 219-238; G.H. Quester, "Offense and Defense in the International System," Transaction Publishers, 2002.
3. S.M. Lynn-Jones, 1995, "Offense-defense theory and its critics," *Security Studies* 4(4): 660-691.
4. C.L. Glaser and C. Kaufmann, 1998, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22(4): 44-82.
5. J. Snyder, 1984, "Civil-Military Relations and the Cult of the Offensive, 1914 and 1984," *International Security* 9(1): 108-146; S. Van Evera, 1984, "The Cult of the Offensive and the Origins of the First World War," *International Security* 9(1): 58-107.
6. Levy, 1984, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis;" P.R. Hensel and S.M. Mitchell (2017), "From territorial claims to identity claims: The Issue Correlates of War (ICOW) Project," *Conflict Management and Peace Science* 34(2): 126-140.
7. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis."
8. M.P. Fischerkeller and R. J. Harknett, 2017, "Deterrence is not a credible strategy for cyberspace," *Orbis*, 61(3): 381-393, M.P. Fischerkeller and R.J. Harknett, 2019, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review*: 267-287.
9. J. Healey, 2021, "Understanding the Offense's Systemwide Advantage in Cyberspace," *Lawfare*.
10. D. Geer, R. Bace, P. Gutmann, and P. Metzger (2007), "Cyberinsecurity: The cost of monopoly."
11. Healey, "Understanding the Offense's Systemwide Advantage in Cyberspace."
12. B. Valeriano and R.C. Maness, 2015, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, New York, Oxford University Press.
13. B. Valeriano, B.M. Jensen, and R.C. Maness, 2018, *Cyber Strategy: The Evolving Character of Power and Coercion*, New York, Oxford University Press; S. Kreps and J. Schneider, 2019, "Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics," *Journal of Cybersecurity* 5(1): tyz007; B. Valeriano and B. Jensen, 2021, *De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War in "Cyber Peace: Charting a Path Towards a Sustainable, Stable, and Secure Cyberspace*. S. Shackelford, F. Douzet, and C. Ankersen (Eds), Cambridge University Press, Forthcoming.
14. B. Valeriano and B. Jensen, 2019, "The Myth of the Cyber Offense: The Case for Cyber Restraint," *Cato Institute, Policy Analysis* (862).
15. E. Gartzke and J.R. Lindsay, 2015, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24(2): 316-348.
16. R. Slayton, 2017, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41(3): 72-109.
17. G. Sartori, 1970, "Concept Misformation in Comparative Politics," *American Political Science Review* 64(4): 1033-1053.
18. E. Nakashima and D. Bennett, 2021, A ransomware gang shut down after Cybercom hijacked its site and it discovered it had been hacked. *The Washington Post*.
19. R. Jensen 2014, "Looking at the extraordinary success of the 'Clockwork Orange': examining the brilliance of total football played by the Netherlands," *Soccer & Society* 15(5): 720-731.
20. S.M. Lynn-Jones, 1995, "Offense-defense theory and its critics." *Security Studies* 4(4): 660-691.
21. Glaser and C. Kaufmann, "What is the offense-defense balance and Can We Measure It?"
22. C. Smythe, 2020, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance." *Yale Journal of International Affairs*, 15: 98.
23. Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.
24. R. Clarke and R. Knake, (2014). "Cyber war," *Tantor Media, Incorporated* Old Saybrook.
25. J. Voo, I. Hemani, S. Jones, W. DeSombre, and A. Schwarzenbach, 2020, *Reconceptualizing Cyber Power*, Belfer Center, Harvard University.
26. N. Kostyuk and Y.M. Zhukov, 2019, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63(2): 317-347.

**NOTES**

27. Valeriano, Jensen, and Maness, "Cyber Strategy: The Evolving Character of Power and Coercion."
28. L. Kello, 2013, "The Meaning of the Cyber Revolution: Perils to theory and statecraft," *International Security* 38(2): 7-40.
29. Levy, "The offensive/defensive balance of military technology: A theoretical and historical analysis," 219-238.
30. Glaser and Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" 44-82.
31. Lynn-Jones, "Offense-defense theory and its critics," 680.
32. M. Montgomery, B. Jensen, E. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano (2020), *Cyberspace Solarium Commission Report*, Washington, D.C.
33. Lynn-Jones, "Offense-defense theory and its critics," 660-691.
34. Y. Gortzak, Y. Haftel, and K. Sweeney, (2005), "Offense-defense theory: An empirical assessment," *Journal of Conflict Resolution*, 49(1): 67-89.  
Glaser and Kaufmann, "What Is the Offense-Defense balance and Can We Measure It?" 44-82.
35. J. Vasquez, 1997, "The realist paradigm and degenerative versus progressive research programs: An appraisal of neotraditional research on Waltz's balancing proposition," *American Political Science Review* 91(4): 899-912; S. Van Evera, 1999, "Causes of War: Power and the Roots of Conflict," Cornell University Press.
37. J. Lindsay, 2013, "Stuxnet and the limits of cyber warfare," *Security Studies*, 22(3): 365-404.
38. S. Applegate, 2012, *The principle of maneuver in cyber operations*, 2012 4th International Conference on Cyber Conflict (CYCON 2012), IEEE.
39. Glaser and Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" 13.
40. J. Healey, 2021, "Understanding the Offense's Systemic Advantage in Cyberspace," *Lawfare*.
41. T. Stevens, 2016, "Cyber security and the politics of time," Cambridge University Press; R. Slayton, 2017, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," *International Security*, 41(3): 72-109.
42. D. Denning, 2015, "Assessing Cyber War" in "Assessing War: The Challenge of Measuring Success and Failure," L. Blanken, H. Rothstein and J. Lepore, Washington, D.C., Georgetown University Press: 266-284.
43. B. Valeriano and R.C. Maness, 2018, "How we stopped worrying about cyber doom and started collecting data," *Politics and Governance*, 6(2): 49-60.



# The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity

---

Dr. Joe Burton

## ABSTRACT

*This article has two aims: first, to examine the future of cyber conflict studies and how the study of cyber security can develop in a more interdisciplinary way; second, to assess the meaning of “offensive” and “defensive” cyber security from the perspective of a variety of different academic disciplines. The article argues that a more holistic and nuanced understanding of cyber offence and defence can be achieved if some of the intellectual silos and disagreements that have characterised the debate so far can be deconstructed and overcome. The article is in three parts. The first section briefly outlines some of the definitional fog that has plagued the cyber security discipline, including over what constitutes cyber offense and defence. The paper then summarises four different subcultures of cyber conflict studies that understand and study cyber security in different ways: International Relations (IR), Political Psychology, International Law, and Computer Science. The concluding section discusses how the cyber conflict studies discipline can move forward, be made more rigorous, and less prone to pathology and dead ends, including through the formation of a cohesive but heterogenous epistemic community.*

© 2022 Dr. Joe Burton



**Dr. Joe Burton** is an Associate Lecturer in the School of International Relations at the University of St Andrews. Prior to that he was a Marie Curie (MSCA-IF) fellow at Université libre de Bruxelles (ULB) where he worked on the two-year European Commission-funded project Strategic Cultures of Cyber Warfare (CYBERCULT) and a Senior Lecturer in the New Zealand Institute for Security and Crime Science (NZISCS), University of Waikato. Dr Burton has worked at the highest levels of professional politics and policy, as an advisor to Cabinet Ministers in New Zealand and the UK, a national campaign coordinator, legislative assistant, researcher, and political organiser. He is a recipient of the US Department of State SUSI Fellowship. Dr. Burton holds a Doctorate in International Relations and a Master of International Studies from the University of Otago, New Zealand, and an undergraduate degree in International Relations from Aberystwyth University in Wales.

## INTRODUCTION

**I**nterdisciplinarity in the study and approach to cyber security has been a regularly stated aim of cyber security researchers and practitioners. Although the immediate and practical protection of computer networks is typically viewed as a job for technical professionals, there are broader social, psychological, political, and legal drivers of cyber conflict and cooperation that are equally important. Despite this being apparent to most in the field, the goal of taking an interdisciplinary approach combining the perspectives of different disciplines, has been a difficult one to achieve. Different lexicons, pedagogies, research methods, and research and policy communities exist. While the emerging discipline of cyber conflict studies has improved its communication and interaction, including at interdisciplinary conferences and through interdisciplinary journals,<sup>[1]</sup> cyber security research and practice continues to be siloed and at times parochial.

This article seeks to reflect on these problems and explore how the discipline might continue to break down barriers between some of the core research areas in cyber security. In doing so the article presents three core arguments. The first is that spending time trying to understand how offense and defense are perceived in different epistemological communities is an important task, especially as attempts to do so are rare.<sup>[2]</sup> Knowing the ways colleagues approach their study of cyber security can help avoid some of the pathologies and silos that have characterised the advancement of the discipline to date. Second, drawing on arguments from the security cultures and strategic culture literature, it is argued that each of the disciplines considered in this article—IR, Political Psychology, Law, and Computer Science—constitute distinct subcultures of cyber conflict studies with their own ideas, ordering devices, narratives, framings, and

behaviours. These subcultures, which have their own frictions and synergies, have emerged over many years, and constitute communities of knowing and understanding cyber security that should be better understood. The third argument relates directly to the future of the discipline. In moving forward cyber conflict studies has the potential to become a more cohesive but heterogenous epistemic community that contains a multitude of perspectives which enhance global security and reduce cyber conflict.

## **1. STUCK IN THE MUD? A SUMMARY AND CRITIQUE OF THE OFFENSE/DEFENSE DEBATE**

The study of cyber security sometimes feels like it is stuck in the mud, unable to move forward, and often mired in stale and unresolvable debates. The tendency to adopt binary (i.e., offense/defense) approaches to complex questions of technology and policy is one example. How and when to act defensively or offensively in cyber security is a difficult question that presents normative and ethical implications and can lead to unintended consequences. The tendency to view complex political, social, and technological questions as a binary is not unique to cyber security. In other fields, the dichotomy between “good and evil,” “right and wrong,” for example, has led to philosophical debates that remain unresolved after centuries. At a technical level, there are many grey areas in cyber security between offense on the one side and defence on the other. The most obvious of these is the idea of “active” cyber defence,<sup>[3]</sup> which to some is a euphemism for offense by any other name while, to others is a set of technical tools—honeypots, for example—that present opportunities to monitor, retaliate or deploy countermeasures against malicious actors.

The lack of clarity in cyber conflict studies stems not only from the tendency to cast debates and policy options in binary terms but from the uncertainty of the domain and the inherent lack of security that both offensive and defensive postures provide. Defense is acknowledged as extraordinarily difficult due to the nature of the technology itself, its ubiquity, the need to supply cheap (and therefore unsecure) cyber products, and the ever-growing attack surface that computer networks provide. On the offense side, the use and development of offensive tools is underpinned by intractable and ongoing geopolitical disputes. These are exacerbated by dynamics within the international system that make it hard to control the spread of offensive cyber capabilities and their malicious use by state and non-state actors, including the growing commercial market in cyber insecurity driven by criminal groups and security dilemmas between nations driven by fear and mistrust.<sup>[4]</sup> Managing a domain that is largely owned and managed by the private sector, which allows for anonymity and covertness and which provides an effective means of subversion and sabotage has proved immensely difficult. The character of uncertainty in cyberspace has wide-ranging effects, including generating fear, the overestimation of cyber risks, and temporal lags in responding to cyber-attacks, including attribution.<sup>[5]</sup> In this environment, acting offensively is no guarantee of a more effective defense, and acting purely defensively is inherently flawed.

Making things worse is the tendency to shoehorn cumulative experiences of insecurity, war, and conflict into the offense/defense debate in ways that are not conducive to peaceful use of ICT or accurate assessment of the present and future of cyber conflict. This occurs through the widespread (mis)use of historical analogies in the field—especially the tendency to link cyber with conventional military operations (cyber pearl harbour) or other security problems, such as terrorism (digital 9/11), and the broader securitization and militarization of the field.<sup>[6]</sup> It also exists in national approaches to cyber security, where countries appear to be approaching cyber security in ways that are deeply conditioned by past actions (often unsuccessfully). For example, the US approach exhibits particular traits that seem to many observers to be unhelpful to enhancing US cyber security—including the desire to project power internationally by using offensive cyber capabilities, to disrupt and deter non state actors beyond US borders, and an exceptionalism that holds that the US has a unique role as a global leader in cyberspace.<sup>[7]</sup> In the military sphere in particular, the dominance of Cold War thinking and the application of military concepts to cyberspace has created inherent insecurities, including the belief that having cyber capability is a deterrent, that cyber tools are effective in creating battlefield “effects,” and that they are effective means of force amplification multiplier or indeed force protection.<sup>[8]</sup> Despite growing scepticism over the utility of cyber as offensive tools,<sup>[9]</sup> and the blowback effects that have been created by using them,<sup>[10]</sup> this type of thinking continues to shape the contemporary cyber security debates in sometimes unhelpful ways.

## 2. SUBCULTURES OF CYBER CONFLICT STUDIES

Approaching the cyber offence debate from the perspective of several different theoretical and disciplinary perspectives is one way to move the debate forward. As argued in this section of the article, each of the key disciplines covered (IR, Political Psychology, Law and Computer Science) offer unique insights into the offense-defense problem, but when combined provide both a better understanding of some of the paradoxes and pathologies in the debate and a path forward to resolving some its intractable difficulties. These disciplines contain unifying ideas and foci that form the basis of distinct subcultures of cyber conflict studies and epistemic communities, defined here as “a network of professionals with recognized expertise and authoritative claims to policy-relevant knowledge in a particular issue area.”<sup>[11]</sup>

### *International Relations (IR) as an epistemic community*

Students and scholars of International Relations are part of a community of knowledge and practice that stretches back to the founding of the discipline after the First World War. This was a conflict of attrition in which a stalemate illustrated that offensive campaigns were not decisive and that defensive measures could create long drawn-out conflicts that inflicted great costs on both sides. The task of IR scholars was to try and address the strategic, ideational, and structural deficiencies and pathologies on which the war was based. During

the Cold War, the discipline's most consuming focus was on managing the perils of nuclear capabilities: how they could be used offensively (and coercively), how to defend against them, and how to find a balance between offense and defense that could provide stability.<sup>[12]</sup>

Because IR is a community of knowledge and practice that shows significant continuities, in which knowledge accumulates, and in which various path dependencies exist, approaches to understanding cyber strategy have followed a similar direction. Scholars have debated cyber coercion,<sup>[13]</sup> cyber stability,<sup>[14]</sup> and the offense-defense balance in cyberspace.<sup>[15]</sup> While there are nuclear lessons for cyber,<sup>[16]</sup> there are also fundamental differences between the management of nuclear and cyber threats. Scholars in the field of IR have tended to lean on old adages and the accumulation of historical knowledge in ways that have not advanced the field enough.

While there are clearly some deep cleavages in the IR community about how to study IR, what to study, and different ontological and epistemological assumptions about some of the key concepts (the divide between realism, liberalism and constructivism has been widely documented, for example), the IR subculture is concerned with a common set of problems and ideas. The first is the nature of power and how it is exercised. Cyber power itself has been analyzed and deconstructed, with a variety of metrics and methods used to study and quantify it.<sup>[17]</sup> A second central and unifying theme that forms the basis of the IR subculture is the notion of explaining both cooperation and conflict under conditions of anarchy.<sup>[18]</sup> According to realist assumptions, cyber defense and offense are responses to an anarchic international environment in which there are no overriding laws or central authority. The covertness of cyberspace lends itself to offensive actions and makes defensive ones very difficult, and its global scope makes sovereign control over it next to impossible, despite recent calls for digital sovereignty in the EU and elsewhere.<sup>[19]</sup> Liberal and constructivist scholarship, conversely, has sought to examine the emergence of international cooperation in the cyber domain, including the establishment of new norms, rights, laws, and institutions. Yet progress has been slow, and norms are easily abrogated in a domain that allows for cheating, covert action and plausible deniability.<sup>[20]</sup>

Critical approaches to IR and security studies have provided further nuance to the field, in part by questioning the nature of power and knowledge in the cyber field, including who it benefits and the political and commercial interests that cyber insecurity serves. Examining the securitisation and militarization of cyberspace<sup>[21]</sup> and how offensive cyber operations are often hyped and framed as existential threats (the digital Pearl Harbor and 9/11 narratives, for example)<sup>[22]</sup> has advanced the field, and the impact of cyber operations on human rights, privacy, and human security have all emerged as significant contributions by IR scholars to the cyber security discipline.

*(Political) psychology and the human factor in offensive and defensive cyber*

Cyber security is not just about technology but about people and their behaviour. This is

the formative premise of a growing literature on the role of psychology and cognitive factors in explaining the interface between technology and the social world. Like IR, psychology is a broad field, but nevertheless contains some core ideas and foci that define it as a subculture and epistemic community within cyber security studies.

Perhaps the closest intersection between cognitive approaches to cyber security and the field of International Relations has been the recognition that some of the concepts IR scholars have been focused on have important cognitive dimensions. The fear created by cyber security discourse and cyber-attacks themselves has been noted by various scholars,<sup>[23]</sup> and people's perceptions, particularly those of policy and decision makers, have impacted how they have reacted to cyber intrusions.<sup>[24]</sup> Scholars have also noted the cognitive schemas<sup>[25]</sup> that exist in policymaking—these are the “mental maps” through which policymakers approach, perceive, and formulate responses to cyber-attacks, and act as an intervening variable between people and the strategic environment in which cyber-attacks take place. These cognitive schemas are distributed culturally and geographically, either in nation-states, or in transnational subcultures, including policy communities, the military, media, and legal community, for example, and contribute to how people in each of these communities react to and comprehend the implications of the inherent uncertainty of the cyber domain.<sup>[26]</sup>

Psychological approaches to cyber security are necessarily and obviously focused on people, and the “human factor” in cyber security has been a recurring theme and an active research agenda. Monitoring human interaction with computers, including detecting anomalous patterns, has also become an important part of securing modern computer networks, which suggests an obvious convergence between Political Psychology and the established field of Human-Computer Interaction. Understanding under what circumstances human mistakes occur, how a user responds to cyber security events and how aware they are of cyber threats and vulnerabilities are important considerations for organisational (and therefore, national) security.<sup>[27]</sup>

The manipulation of human targets has also been integral to many modern cyber security breaches. As Hatfield argues, the social engineering concept had its origins in politics (and intelligence studies), thus providing another important link between psychology and political science approaches to security, and is based on the principle of epistemic asymmetry.<sup>[28]</sup> That is to say, the people (hackers) who manipulate the victims have a higher degree of knowledge about how the platforms work and are able to stretch and alter the behaviour of their targets through deception. This form of technocratic dominance<sup>[29]</sup> is also key to understanding the evolution of the computer science epistemic community, as detailed in a subsequent section.

### *Legalism in a legalistic community*

Colin Gray noted the existence of subcultures with the US that had an influence on US

strategic doctrine during the Cold War, noting that there was a community of lawyers, in the State Department and elsewhere, to whom the use of force was an anathema.<sup>[30]</sup> This legalistic community was predisposed to thinking about international affairs in legal terms and in the context of laws, treaties and regulatory mechanisms. In the current cyber security field, legal scholars have coalesced around a set of ideas and approaches to cyber conflict which exhibit an attachment to key ideas. This cyber legalism has had a positive impact on cyber security practice and policy but failed at the international level to bring meaningful advances to cyber security.<sup>[31]</sup>

The cyber legal subculture has been naturally predisposed to a focus on norms and laws for the obvious policy reason that nations and academia have needed to understand how international law might apply to complex computer networks that are opaque and favour covert action. Cyber commanders in the military sector, for example, have needed to know when a use of a cyber-attack or operation may be illegal. International law has also been driven by operational needs. The Tallinn Manual process has been foremost in the effort to map out how existing international law might apply to cyber conflict during war, and outside of armed conflict.<sup>[32]</sup> There have also been sustained effort at the UN level to promote and agree on international cyber norms through the OEWG and GGE processes. While these efforts have yielded some progress, there is a growing frustration in the field around the triumphalism surrounding UN level agreements, when nations that are agreeing to be bound by norms are (a) flagrantly violating them from the outset, or (b) failing to implement them.<sup>[33]</sup> Debates over the potential negotiation of a digital Geneva convention are but one example. Some legal scholars have endorsed the idea that there is no need for a convention to protect civilians against cyber-attacks when the Geneva convention, they argue, already does. Such an approach, however, may limit the emergence of new agreements with greater specificity which encourage buy-in and adherence from states and the tech sector, including more sophisticated and holistic verification and accountability measures.<sup>[34]</sup>

These challenges are not just practical problems, they are cultural ones, stemming from the culture of legal approaches from western nations in particular.<sup>[35]</sup> As analysis by Ross reveals, legal culture tends to lean towards the concept of precedent, which is difficult to establish in cyber security because of the unprecedented nature of cyber technologies, but nevertheless is used as a tool by the legal community to stabilize the seemingly chaotic and controllable nature of cyberspace.<sup>[36]</sup> In these ways, the legal profession's pre-existing ideas, behaviours and practices shape its response to the challenge of securing cyberspace.

### ***Computer science, network defense and offensive cyber***

While there is a risk of assigning an identity to the technical cyber security community, which is broad and diverse, there are also some potentially binding characteristics that constitute a more technically-oriented subculture and epistemic community. The first is an attachment to freedom of information and an aversion to processes that create restrictions

to the flow of data. This is a bedrock principle that underpins the development of modern computing. This has obvious implications for cyber offense and defense – offensive measures can be used to liberate information and defensive measures to protect or impede access to information. Tensions between the values associated with a free and open Internet on the one hand and national security requirements on the other are therefore cultural and technical.

Second, the computer science epistemic community is built on valuing technical expertise and skills and the diffusion of that expertise within a technical community. Although the same could be said of other disciplines, the technical and scientific knowledge that forms the basis of advances in software, hardware and networking technology is not widely shared in society and is deemed of particular value. The idea that computers are a complex technology that wider society or indeed the policy making community does not understand is a bedrock notion in this culture. It also forms part of digital knowledge gaps that continue to be problematic across both academic and policy communities.

This feeds into a wider behavioral characteristic of the cyber security technical community that relates to the tools and technology itself and how it is used. Technical experts might be reluctant to acknowledge this point, but widespread in the subculture is the idea that computer technology is designed to be broken, probed, tested, deconstructed, or hacked. By this logic, understanding what makes computers work involves taking them apart or indeed breaking them. There is status in finding bugs (and bounties now paid for them) and a performative element to major breakthroughs in exploits. Of course, much of this process is necessary to test the technology before or after commercial release and ethical hacking and penetration testing has resultantly become a big industry. But it has also encouraged the profusion of knowledge and skills about how to subvert computer networks that has, in some cases, contributed directly to cyber insecurity. Paradoxically, the profusion and advancement of hacking skills for the purposes of defense has created more vulnerabilities and a more widespread skillset that is being adopted and used to hack into computers for malicious reasons. While there is little technical distinction between defensive security testing and offensive hacking, the intent, behaviour, and results of this behaviour is paramount to understanding modern cyber insecurity.

Finally, an integral part of the cyber security technical subculture which directly influences how offense and defense is understood and practiced is a reticence to have the technology regulated or controlled. The idea that underpins the culture is that technology should be democratising, in the sense of being in the hands of the people. Governments should not be involved in controlling the technology and technology itself is often uncontrollable – it is outside of the capacities of policymakers or legislators to bring about meaningful regulation. The widespread use of ransomware technology fuelled by bitcoin, a technology that is difficult to regulate, and the growing market in spyware or surveillance technology are illustrative examples. This has obvious implications for relationships with other subcultures, as

Internet technologies are disruptive to existing power dynamics and particularly the pre-eminence of the state and meanwhile poses distinct and direct challenges to international law.

### **3. THE FUTURE OF CYBER CONFLICT STUDIES - TOWARDS A SINGLE EPIS- TEMIC COMMUNITY**

One of the challenges of writing an article covering four complex disciplines, each with many and diverse subfields them, is brevity and over-generalization. The principal elements of each of the subcultures presented above are instrumentalist ones that speak to policy-relevant expertise. The salient point here is that a complete picture of cyber conflict can only be gained by understanding the limitations of each discipline and by learning from the others. In designing cyber security education and advancing research in cyber conflict studies, scholars should pay close attention to what other disciplines offer and the limitations of their own field.

In building a more interdisciplinary approach to cyber conflict studies, what obstacles and impediments are there? Can the silos between subcultures be overcome, and could a single cyber security subculture emerge which is based on shared ideas and mutual understanding?

The first problem here is a political and organizational one within academia. The debate about which subjects and disciplines should be given priority, resources, and funding, is contentious and continuing. Debates about cyber security education take place in a context where humanities and social sciences are not always (or often) funded to the same levels as compared with STEM disciplines; there is pressure on social science and humanities to do more technologically/scientifically focused work, and not always the same pressure on technologists to think more broadly about policy, strategy, or even the psychological dimensions highlighted in this piece. Again, this is a cultural problem exacerbated by diverging ideas and perspectives, the creation of insiders and outsiders, and a behavioral failure to create joint programs, centers, degrees, and training. Weston argues, "In a world that is rapidly progressing with new technologies, being 'outside' of STEM is a bit like being driven around in a car while being forced to sit in the back seat."

These problems are present in funding, ranking, and publishing models, too. IR cyber conflict scholars, for example, will generally receive less credit for publications in journals outside their fields than for publishing in the top IR journals. The UK's Research Excellence Framework has only recently introduced guidelines for accurate and fair assessment of interdisciplinary and collaborative research.<sup>[37]</sup> This problem pervades the organization of universities which are often structured around siloed departments as opposed to research centres and institutes that encourage collaborative research. Some progress is being made here. For example, the UK Centres of Excellence model for cyber security recognizes the interdisciplinary nature of the field. As this article suggests, however, a broader cultural

change will be needed to move the cyber conflict studies field on from some of its limitations and pathologies.

A second obstacle to developing effective multidisciplinary education has to do with research methods and their incorporation into a cohesive whole. The need to blend quantitative approaches with qualitative ones is a challenge and combining the methods of four or more different fields is an even bigger one. As Mulvenon argues, “the field of cyber conflict must sample from a wide variety of methodologies and tools.”<sup>[38]</sup> Relatedly, finding a common language or lexicon across disciplines is a challenge. In the IR discipline deterrence is a military concept closely associated with the Cold War context and nuclear weapons while in law, it is a legal framework; in psychology, it is about changing the thinking of an attacker – and influencing their psychological decision-making processes. Similarly, in the technical sector, policy is mostly understood as organizational policy, for example, restricting use of USB drives in the workplace. In contrast, government officials and IR scholars understand policy to be about the government’s overall direction in cyber security—whether to develop offensive cyber capabilities in the military, for example, or institute mandatory reporting of cyber incidents. Finding a common understanding of language in diverse multinational research and policy environments will be difficult even when integral to a more secure cyberspace.

A further challenge is the need to continue to diversify the field. To pose a provocative question: is cyber conflict studies introducing pathologies into analysis because it is largely male, western, and white? IR is undergoing a reckoning with its inherent biases and colonial assumptions increasingly questioned. The debates about the role of race in securitization theory, and the lack of engagement with theory and practice from the global south has been highlighted.<sup>[39]</sup> The cyber conflict studies field has yet to engage meaningfully with these problems. The lack of gender balance and ethnic diversity in the field is being challenged and addressed by groups like Women in Cyber Security and other initiatives that advance and mentor underrepresented scholars in the field. While commendable, at the present stage this is window dressing for a more deep-rooted problem—that our approach to cyber insecurity contains a larger epistemological and ontological blind spot to diversity issues.

Creating an environment of reciprocity rather than rivalry between disciplines and scholars is a related issue. This article has been deliberately provocative in pointing out some of the pathologies that exist across the disciplines covered. Yet, unless we collaborate with cyber security professionals from outside of our disciplines, these basic differences in understanding or key terms will not be recognized or overcome. A four-way (at least) street between disciplines is needed where computer scientists, for example, learn about politics and policy issues, and IR scholars learn about the technical aspects of computer science. The need to upskill in areas outside of our own immediate disciplines should be mutually invested in and a reciprocal process. Embedding modules/classes/lectures on the technical aspects of cyber security in policy/IR courses and vice versa is an immediate and low-hanging solution to addressing this problem.

Finally, resourcing a multidisciplinary approach in ways that builds a more cohesive discipline will be important. Not all educational institutes will have the resources to do this well. A concern here is that the richest institutions with the most students create the programs that become a benchmark, which in-turn leads to a further stratification of the education system, with a few elite institutions dominating in a particular area. Creating interdisciplinary programs requires leadership, strategic hiring decisions, strategic funding, and sometimes the restructuring of subsidiary programs. Educational cultures can be resistant to change and slow to adapt. Conversely, requiring computer science students to take political science courses, or psychology courses may lead them to sacrifice essential skills they need to cover in their own discipline.<sup>[40]</sup> Another issue relates to flexibility and heterogeneity. There appears to be merit in developing common approaches to cyber security, but a one-size-fits-all approach may harm some of the cultural diversity that currently exists within the field. Merging or consolidating subcultures could provide beneficial in some ways but maintaining diversity of thought in understanding the future of offense and defense will be critical too. The future of cyber conflict studies thus arguably lies in creating a heterogeneous epistemic community rather than a homogenous one.🛡️

*Research for this article received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 844129.*

## NOTES

1. The *Journal of Cyber Policy*, *Journal of Cyber Security*, and *The Cyber Defense Review* are prominent examples.
2. For a notable and commendable example, see J.S. Blair, A.O. Hall, and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," in *Computer*, vol. 52, no. 3, pp. 58-66, March 2019, doi: 10.1109/MC.2018.2884190.
3. For a definition of Active Cyber Defense and an exploration of its meaning, see R.S. Dewar, 2014, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence." *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, *Cyber Conflict (CyCon 2014)*, 2014 6th International Conference On, June 7–21, Doi:10.1109/CYCON.2014.6916392.
4. B. Buchanan, 2016, *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press.
5. Monica Kaminska, Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021.
6. See Joe Burton & Clare Lain, 2020, Desecuritising cybersecurity: towards a societal approach, *Journal of Cyber Policy*, 5:3, 449-470, DOI: 10.1080/23738871.2020.1856903.
7. J. Burton, 2021, 'Defending forward' through 'Persistent Engagement': Assessing the Strategic Cultural Determinants of US Cyber Security Strategy,' Paper presented at BISA US Foreign Policy working group.
8. M. Smeets, 2018, The Strategic Promise of Offensive Cyber Operations, *Strategic Studies Quarterly*, 12(3), 90–113, <http://www.jstor.org/stable/26481911>.
9. B. Valeriano and R.C. Maness, 2015, *Cyber war versus cyber realities: Cyber conflict in the international system*, Oxford University Press, USA.
10. J. Radack & W. Neuheisel, 2021, SolarWinds Is Not the 'Hack of the Century.' It's Blowback for the NSA's Long-time Dominance of Cyberspace, <https://www.commondreams.org/views/2021/01/27/solarwinds-not-hack-century-its-blowback-nsas-longtime-dominance-cyberspace>.
11. <https://www.britannica.com/topic/epistemic-community>.
12. R. Jervis, 1979, Why Nuclear Superiority Doesn't Matter. *Political Science Quarterly*, 94(4), 617–633, <https://doi.org/10.2307/2149629>.
13. B. Valeriano, B.M. Jensen, and R.C. Maness, 2018, *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford University Press.
14. F.D. Kramer, 2012, Achieving international cyber stability, *Georgetown Journal of International Affairs*, 121-137.
15. Rebecca Slayton, What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, 2017; 41 (3): 72–109. doi: [https://doi.org/10.1162/ISEC\\_a\\_00267](https://doi.org/10.1162/ISEC_a_00267).
16. Joseph S. Nye, Jr., 2011, Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5(4): 18-38.
17. <https://www.iiss.org/blogs/-paper/2021/06/cyber-capabilities-national-power>.
18. See J. Lindsay, presentation to Hague conference on cyber norms, November 2021.
19. Frances G. Burwell and Kenneth Propp, 2020, The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>.
20. A. Grigsby, 2017, The end of cyber norms, *Survival*, 59(6), 109-122.
21. J. Burton & C. Lain, 2020, Desecuritising cybersecurity: towards a societal approach, *Journal of Cyber Policy*, 5(3), 449-470.
22. S. Lawson, 2013, Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats, *Journal of Information Technology & Politics*, 10(1), 86-103.
23. M.A. Gomez and E.B. Villar, 2018, Fear, uncertainty, and dread: Cognitive heuristics and cyber threats, *Politics and Governance*, 6(2), 61-72.
24. Ibid.
25. M.A. Gomez, 2021, Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas, *Defence Studies*, [Online] 21 (1), 25–46.
26. Aaron F. Brantly, Risk and uncertainty can be analyzed in cyberspace, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab001, <https://doi.org/10.1093/cybsec/tyab001>; M.A. Gomez (2021) Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas, *Defence Studies*, 21:1, 25-46, DOI: 10.1080/14702436.2020.1851603.

**NOTES**

27. B.M. Bowen, R. Devarajan, and S. Stolfo, 2011, November. *Measuring the human factor of cyber security*, In 2011 IEEE International Conference on Technologies for Homeland Security (HST) (230-235), IEEE.
28. J.M. Hatfield, 2018, Social engineering in cybersecurity: The evolution of a concept, *Computers & Security*, [Online] 73, 102–113.
29. Ibid, 104.
30. Colin S. Gray, "National Style in Strategy: The American Example." *International Security* 6, no. 2 (1981): 21-47; Colin S. Gray, *Nuclear Strategy and National Style* (Lanham, Md.: Hamilton Press, 1986), 22.
31. Lucas Kello, Cyber legalism: why it fails and what to do about it, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab014, <https://doi.org/10.1093/cybsec/tyab014>.
32. <https://ccdcoc.org/research/tallinn-manual/>.
33. For a discussion on implementation of cyber norms, see Kerttunen, M. and Tikkanen, E. (2021), Putting Cyber Norms Into Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies, available: <https://cybilportal.org/wp-content/uploads/2021/11/Putting-Cyber-Norms-in-Practice.pdf>.
34. J. Guay and L. Rudnick, (2017), What the Digital Geneva Convention means for the future of humanitarian action, UN-HCR, <https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/>.
35. R. Ross, 2002, Communications Revolutions and Legal Culture: An Elusive Relationship, *Law & Social Inquiry*, 27(3), 637-684. doi:10.1111/j.1747-4469.2002.tb00822.x.
36. Ibid, 641.
37. Research Excellence Framework, 2021, Interdisciplinary Research, <https://www.ref.ac.uk/about/interdisciplinary-research/>.
38. J. Mulvenon, 2005, Toward a cyberconflict studies research agenda. *IEEE Security & Privacy*, 3(4), 52-55.
39. A. Howell and M. Richter-Montpetit, 2020, 'Is securitization theory racist? Civilizationism, methodological whiteness, and antiblack thought in the Copenhagen School,' *Security Dialogue*, 51(1), 3–22, doi: 10.1177/0967010619862921; Amitav Acharya and Barry Buzan, *The Making of Global International Relations: Origins and Evolution of IR at Its Centenary*, Cambridge University Press, 2019.
40. Fred S. Roberts, The Challenges of Multidisciplinary Education in Computer Science, *Journal of Computer Science and Technology*, Beijing Vol. 26, Iss. 4, (July 2011): 636-642.



# Winning Future Wars: Russian Offensive Cyber and Its Vital Importance

*in Moscow's  
Strategic Thinking*

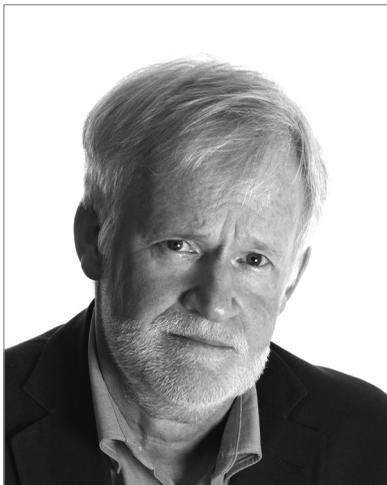
Dr. Rod Thornton

Dr. Marina Miron

## **ABSTRACT**

*This article highlights the importance of offensive cyber as an instrument for Russia to generate strategic effect against NATO and its core states. It focuses on the use of offensive cyber by the Russian military at the strategic level. This military is perceived to be the lead actor in the operationalization of offensive cyber by Moscow. Because the Russian military sees itself at an overall disadvantage vis-à-vis NATO's conventional capabilities, it is offensive cyber that it is looking to provide a means of fundamentally redressing this imbalance. Offensive cyber is a vital tool for the Russian armed forces. It is indeed viewed as being the only available instrument that can, short of the use of nuclear weapons, bring about the neutralization of core NATO states; that is, to defeat them. This neutralization can be engendered, according to Russian military logic, in two ways: either through cyber-psychological or cyber-technical attacks. This article unpacks these terms and indicates how both can theoretically generate the degree of impact that could lead to the neutralization of core NATO states. Finally, there will be a review of the Russian use of offensive cyber in the Ukraine conflict.*

© 2022 Dr. Rod Thornton, Dr. Marina Miron



**Dr. Rod Thornton**, formerly in the British Army, teaches at the UK Defence Academy as a member of the Defence Studies Department of King's College London. A Russianist by academic background (having lived and worked in both Moscow and Kyiv), his research today focuses mainly on the Russian military, including its cyber capabilities. He has written widely on various aspects of the Russian military and teaches high-technology weapons systems at the UK Defence Academy.

## INTRODUCTION

This article analyses the concept of offensive cyber when employed at the strategic level by the Russian military against core NATO states. The focus here is on understanding how important offensive cyber is to the strategic thinking of the Russian military and to Russia itself. Offensive cyber is viewed as the country's only truly war-winning tool when it comes to confrontations with actual NATO states (rather than more limited conflicts such as Ukraine).

The Russian military seeks to employ offensive cyber in two forms. The first is what is referred to in Russian as the cyber-psychological (*kiber-psikhologichkii*). This form is being widely utilized now against NATO states in considerable depth as part of what has been described in United Kingdom government documents, and even before the Ukraine war (which is discussed below), as the "intensifying geopolitical competition" between Russia and NATO states.<sup>[1]</sup> This competition is currently characterized by restraint and conducted in the "sub-threshold"<sup>a</sup> space.<sup>[2]</sup>

From the Russian perspective, offensive cyber-psychological activities in this sub-threshold competition are important because they can be used to manipulate people's minds – from political figures to entire populations. The core belief in Russian military circles is that offensive cyber tools, when used as a weapon of psychological influence, can over the long term and through a process of weakening, destabilizing, and undermining from within, go so far as to defeat (or "neutralize," to borrow from the Russian military lexicon) Moscow's peer-state adversaries. This can be done without a shot being fired. Once neutralized, such adversaries, and considering Clausewitz's understanding of how wars are won,<sup>b</sup> can be subject to the imposition of [Russian] will, whether they are conscious of it or not.

a Sub-threshold activities are those that do not push a targeted state into a kinetic response, i.e., that do not incite armed conflict.

b For Karl von Clausewitz, the aim of war is to "compel our enemy to do our own will" (Clausewitz 1989: 75).



**Dr. Marina Miron** is an honorary research fellow at the Defence Studies Department, King's College London. She is also a member of the Centre for Military Ethics, King's College London. Her current research focuses on emerging and future military technologies, including drones, human augmentation, artificial intelligence, and cyber instruments, and how these impact the strategic and operational landscapes. As well as producing several publications, she has participated in numerous conferences related to cyber and information warfare and has presented on the topic at the UK MoD. Dr. Miron is currently working on a UK MoD-funded project related to the integration of human augmentation technologies in the military.

Cyberattacks in this context form a vital element in the Russian military's current strategic application against Western actors of what it refers to as its sub-threshold "active defense" (*aktivnaya oboronna*) measures. Active defense entails using predominantly non-kinetic means which are designed to fundamentally weaken NATO state adversaries and the whole Alliance structure. This notion of active defense and the important role of cyber-psychological attacks in creating the neutralization will be highlighted in this article.

The second strand of Russian offensive cyber comes in the "cyber-technical" (*kiber-tekhnicheskii*) form. This form is generally understood in the West to represent cyberattacks. These will be conducted against NATO states' information technology (IT) infrastructure and technical systems. In line with the "active defense" logic, these attacks are currently kept at a low level so that they remain definitively sub-threshold. However, if (or when?) the era of competition with NATO moves into one of very high international tension or even of actual inter-state conflict, restraint will no longer have any currency and then the genie may truly come out of the Russian military's offensive cyber-technical bottle. A series of cyberattacks that target adversary states' major IT systems can, in this scenario, coalesce to mean that such states, again undermined from within, may no longer be able to function as states. The cyber-technical attacks can, like their cyber-psychological brethren, become a truly war-winning weapon over a much shorter time frame. The shock and devastation wrought by a synergistically applied set of cyber-technical attacks can, as some Russian observers have noted, create effects akin to those of nuclear weapons.<sup>[3]</sup>

As this article emphasizes, it is essential to appreciate how much the Russian military strives to create cyber-technical attacks aimed at creating immense shock and devastation. As a cultural norm, the military sees that *all* engagements from the tactical level to the

strategic as being won most efficiently against strong opponents by striking a surprise blow of stunning, crushing power. This blow, derived from the thinking of the Soviet era, is known as the *udar*. This is noted as being a “concept rarely used in Western military thought.”<sup>[4]</sup> But as Shimon Naveh expresses it, the *udar* is “one of the fundamentals of Russian military thought.”<sup>[5]</sup> The shock of a well-conceived and effectively applied *udar* is one from which any adversary, be it a platoon on a battlefield or a state actor, cannot recover. The *udar* is the best way of “neutralizing” Russian adversaries.<sup>[6]</sup>

In this article, we explore why the two forms of offensive cyber—cyber-psychological and cyber-technical—hold such important places in Russian strategic thinking, both now and particularly in the near- to medium-term future. It could be the case that Russian offensive cyber may pose, in terms of strategic risk, the greatest short- to medium-term threat to both individual NATO states and the coherence of the Alliance itself. China may represent a long-term threat to the US and its allies, but Russian offensive cyber is far more the enemy at the gate.

This article engages mainly with Russian *military* writings on offensive cyber. It is perceived that this military<sup>c</sup> (and those associated with it, for example, the non-state hacker groups it employs)<sup>[7]</sup> is both the major player in terms of the Russian state bodies engaging in offensive cyber (through the military’s intelligence arm, the GRU<sup>d</sup>) and also the prime mover in coordinating the activities of the state’s other offensive cyber protagonists.<sup>[8]</sup> These are the internal security force, the FSB<sup>e</sup> and the SVR<sup>f</sup>, the foreign intelligence service.<sup>[9]</sup> The head of the Russian military (at the time of writing), General Valerii Gerasimov, also gives the impression that it is his military that the coordinating body for the state’s offensive cyber actors.<sup>[10]</sup>

### *Russia’s strategic position as viewed from Moscow*

To truly understand the vital and growing importance of offensive cyber in the Russian strategic picture, some background is required. The Russian military views offensive cyber as an essential means of providing profound strategic effect in a geopolitical environment where Moscow sees itself as being under significant threat from the West and NATO with few if any, available means of effectively countering this threat.<sup>[11]</sup>

This Western threat is said to be evidenced by a bellicose NATO (or collections of NATO countries), which has engaged in a series of post-Cold War interventions in Iraq, Bosnia, Kosovo, Afghanistan, Libya, and Syria. These stood counter to Moscow’s strategic interests. Second, of course, there has been the gradual expansion of NATO to Russia’s borders. Perhaps more significant, though, has been NATO’s encouragement over recent years of Georgia and, more especially, Ukraine to join the Alliance. Leading Russian politicians and military figures have long been pointing out that NATO’s behavior represents a direct threat to Russia and Russian

<sup>c</sup> This is also a military that has recently become Putin’s most favored organ of state defense and security.

<sup>d</sup> Technically, the GRU [Glavnoe Razvedyvatel’noye Upravleniye] (Main Intelligence Directorate) is today the GU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation), but the name GRU seems to have stuck.

<sup>e</sup> Federalnaya Sluzhba Bezopasnosti [Federal Security Service] operates using the APT28 group (including Cozy Bear) and others such as Turla and Palmetto Fusion.

<sup>f</sup> Sluzhba Vneshnei Razvedki [Foreign Intelligence Service] operates using the APT29 group.

interests.<sup>[12]</sup> This idea of being at a disadvantage is strongly reflected in the Russian *Military Doctrine* of 2014<sup>[13]</sup> and even more so in the *National Security Strategy* of July 2021.<sup>[14]</sup> This sense of both threats is heightened, moreover, by the acknowledgment—and made apparent in the opinions expressed by General Gerasimov and other leading figures in Russian political and military spheres—that NATO is capable of fielding armed forces that are both qualitatively and quantitatively stronger than Russia.<sup>[15]</sup> The prognosis is that if any major shooting war with NATO itself does take place, then the Russian military is likely to lose heavily.<sup>[16]</sup> The follow-on from this sense of both threat and vulnerability is that Moscow's freedom of action is being constrained on the international stage. There is a feeling within Russia that the country's ability to act as a great power wielding significant influence on world events—which Moscow feels to be its rightful destiny—is being thwarted by the activities of a more powerful NATO.<sup>[17]</sup>

### *The actual nature of the threat*

This general background threat is manifest, in Russian eyes, in two specific forms of direct jeopardy from the NATO quarter. The first comes in a kinetic form. This will be specifically exhibited, the judgment is, not so much from a nuclear attack (which is considered highly unlikely in Russian circles)<sup>[18]</sup> but rather from a surprise strike against Russia using the United States' nascent Prompt Global Strike (PGS) system (*Global'nii Udar* in Russian).<sup>[19]</sup> This consists of (according to Russian estimates) some 6,000 or so non-nuclear cruise missiles based on US surface and sub-surface vessels. Russian analysts fear these missiles could be launched *en masse* and at any time against the country's critical national infrastructure (CNI) and, literally overnight, largely destroy it. Russia could only retaliate by going nuclear, which is a decision the Kremlin does not want to contemplate.<sup>[20]</sup> However nascent it might be, a potential strike by the PGS system is still seen to represent an existential threat to the Russian state. It is noted, indeed, as being the “most serious threat facing Russia.”<sup>[21]</sup>

A second existential threat that NATO is seen to pose comes in a non-kinetic form. This is the fear of a NATO-inspired color revolution that would threaten the political regime in Moscow. This is where Western soft power would be used as a weapon to weaken and destabilize Russia.<sup>[22]</sup> With the perceived Western control of the Internet and leading social media platforms, the Kremlin looks upon its population as being bombarded with favorable views of both the West and of those Russian agencies and political figures who oppose Putin and his government. These same Western sources likewise carry negative portrayals of Putin and his government. The concern is that such messaging has caused and will continue to cause domestic social unrest in Russia that may remove Putin from power.<sup>[23]</sup>

With these twin threats posed by a surprise PGS strike and a color revolution and set against a background of perceived long-term NATO bellicosity, there is a sense within Russia's civil and military hierarchy that NATO and the West more broadly, is already engaged in the form of competition that is akin to an actual (albeit non-kinetic) war with Russia. And it is a war in which Moscow feels it is at a distinct disadvantage. It has a weaker military (one getting weaker

by the day in Ukraine); it cannot match the PGS system, and it does not have the influence inherent in Western soft power. NATO thus has ways of potentially “neutralizing” Russia or of imposing its “will” on the country that Moscow cannot reciprocate with.<sup>[24]</sup>

### *The Russian response*

The Russian response to these perceived threats appears focused on ensuring that NATO and its leading states are, above all, never in a position to take any decision to use any form of armed force against Russia. This is mostly about shaping mindsets within NATO countries. The first element here is to employ traditional deterrence. Russia has recently been beefing up its nuclear capability. The message is one that deterrence by punishment still exists in the nuclear realm.<sup>[25]</sup> Russia has also increased its territorial defense, notably through the establishment of what is known in the West as anti-access/area denial (A2/AD) bubbles around the country’s borders.<sup>[26]</sup> These consist of a series of defensive weapons systems, which mostly rely on air defense and anti-missile missiles. These A2/AD arrangements are, in large part, designed to thwart the PGS system and thus generate deterrence by denial.<sup>[27]</sup>

However, while such an enhanced nuclear capability and the A2/AD defenses might deter NATO policymakers from contemplating a physical attack on Russia (which has been discussed in a 2018 U.S. Army doctrinal publication),<sup>[28]</sup> they do not offer the possibility of Russia prevailing—winning—in the ongoing non-kinetic competition/war or any future actual kinetic one with NATO forces. What Moscow feels it needs are tools that can put NATO and its core states themselves under threat.

Russian military writings ponder this situation. There is a need to find the most apposite ways to weaken and destabilize core NATO states and to undermine the Alliance’s coherence so that they both are no longer able to threaten Russia physically or to stand together to stymie Russian geopolitical interests.<sup>[29]</sup> In essence, as stated by one Russian analyst, NATO must be “brought into a state where they can no longer fight.”<sup>[30]</sup>

It is argued that a degree of aggression or “pre-emptive neutralization” as Gerasimov calls it, is advocated for here.<sup>[31]</sup> Still, this aggression must remain sub-threshold so as to not incite retaliatory kinetic action by NATO. Ideally, it should also be deniable so the blame for any aggressive acts should not fall on Russia.<sup>[32]</sup> The degree of sub-threshold aggressiveness currently generating this process of weakening is captured in the military’s aforementioned new strategy of “active defense” [*aktivnaya oborona*].

### *Active defense*

The necessity to specifically adopt active defense was first voiced by Gerasimov in a speech in March 2019.<sup>[33]</sup> It is a strategy that is currently being enacted by his military in the sub-threshold space in coordination with other Russian security actors. It utilizes a variety of measures, including diplomatic and economic activities and attempts to alter election results

in Western states.<sup>[34]</sup> Also included are saber-rattling troop movements. As Gerasimov states, “demonstrations of military power [will] enhance the effectiveness of non-military [active defense] means.”<sup>[35]</sup>

There is an argument that these active defense measures are nothing new; merely a continuation of the traditional Soviet military’s sub-threshold idea of *aktivnost* ‘ (basically, activity)<sup>[36]</sup> and the KGB’s past ‘active measures.’<sup>[37]</sup> But there is something more here. Active defense today is more muscular, bellicose, and refined than its predecessors. Indeed, one renowned Russian observer of the military, Pavel Felgenhauer, has noted that Gerasimov’s active defense strategy actually represents a step up in aggressiveness from what previously had been labeled as the “Gerasimov Doctrine” of 2013.<sup>[38]</sup> This was Gerasimov’s original call for his military to engage in more belligerent non-kinetic actions against Western adversaries.<sup>[39]</sup> According to Felgenhauer, Gerasimov’s new and even more belligerent idea of active defense should now be called “Gerasimov 2.0.”<sup>[40]</sup>

One area of active defense that highlights this increased aggression is in the field of information warfare. And it is information warfare that appears, from the Russian perspective, to be the most effective element of active defense. Today, information warfare offers more than it ever did as a weapon. It offers the ability to neutralize state adversaries but with very little outlay or expense and with little fear of facing retaliatory action.<sup>[41]</sup> For a vulnerable Russian—from Moscow’s perspective—and with few instruments to mitigate this vulnerability, information warfare is seen as having a truly vital *strategic* role.<sup>[42]</sup> Gerasimov has said specifically that “the study of issues of preparation and conduct of information actions is *the most important task of military science* [emphasis added].”<sup>[43]</sup> Thus, it is not hypersonic missiles or artificial intelligence, or any other new technology that Russian military science should focus on, actually it is information actions.

### ***The crucial aspect of information warfare***

It is notable in Russian military literature just how much information warfare (IW) as a topic stands out. There are many discussions about using information as a weapon from the tactical level to the strategic.<sup>[44]</sup> Again, this is nothing new. The Soviet military previously placed a great deal of emphasis on the use of information as the core element of its psychological warfare activities.<sup>[45]</sup> Western militaries, of course, both in the past and very much so still today, are more wary of engaging in psychological operations, particularly at the strategic level.<sup>[46]</sup> Thus there is far more discussion within the Russian military regarding the use of IW<sup>[47]</sup> at both the operational level and, particularly, the strategic, that is simply not apparent within the militaries of Western states.<sup>[48]</sup>

This military’s understanding of IW can be judged using the recent definition supplied by one of the current leading writers on Russian strategic thinking, Aleksandr Barthosh:

A set of measures taken to achieve information superiority over the enemy by influencing his information systems, processes, computer networks, the public and the individual consciousness and subconsciousness of his population and personnel of his armed forces while protecting one's own information environment.<sup>[49]</sup>

This definition captures the general Russian view that information warfare encompasses attacks on computer networks and the consciousness and subconsciousness of civil populations and military personnel. The Russians break down IW into two mutually supporting elements: information operations and cyber operations.<sup>[50]</sup> The concept of cyber operations – or offensive cyber<sup>g</sup> – is then further broken down into the two distinct strands: cyber-technical and cyber-psychological.<sup>[51]</sup>

These offensive cyber operations, of course, tick all the boxes required of a Russian military active defense measure: they are sub-threshold; they are (theoretically) deniable, and they can, especially in the current era, have a considerable effect. Moreover, as noted, the Russian military sees offensive cyber as leading to the weakening and destabilizing of adversary states, and possibly to their outright defeat. Here lies the true importance of offensive cyber for Russia: it appears to offer its *only* truly war-winning weapon against NATO as a collective and against its principal state actors.<sup>[52]</sup> The Russian belief, moreover, is that such war-winning results can be achieved using either of the two strands of cyberspace operations, the cyber-psychological or the cyber-technical.

### ***Cyber-psychological operations***

Russian cyber-psychological operations at the strategic level and applied in the geopolitical environment of competition involve the use of the Internet, and especially social media platforms, to spread propaganda/black propaganda and misinformation/disinformation that can alter perceptions in targeted states across a broad political and societal range.<sup>[53]</sup> Sergei Naryshkin, the head of the Foreign Intelligence Service (the SVR) – where the SVR is a major player in Russian cyber-psychological operations<sup>[54]</sup>– expressed the general understanding as to the merits of cyber-psychological operations:

The modern world is characterized by the fact that non-military conflicts are multiplying, and their main targets are not armed forces or military facilities, but government agencies, the political structure of societies, vital resources, and, finally, social consciousness.<sup>[55]</sup>

This form of offensive cyber, when applied over a sufficiently long timeframe, is designed to lead to a slew of outcomes positively judged by Moscow. At one end of the spectrum, cyber-psychological operations would focus on changing the decision-making calculus of leading political figures in targeted states in ways desired by Moscow. Here the aim would be to create an effect according to the long-established Soviet/Russian desire to seek strategic advantage by engaging in reflexive control measures. This is where Western politicians and military leaders would be manipulated by Russian informational inputs without their realizing it.<sup>[56]</sup> Cyber-psychological interventions can also alter the actions of governments by

g There is no specific Russian term for offensive cyber.

creating groundswells of public opinion that generate pressure on administrations. They can also involve attempts to affect election results using misinformation/disinformation.<sup>[57]</sup>

More dramatically, though, cyber-psychological operations are seen as moving beyond mere influence or manipulation to fundamentally destabilize adversary states. A chief target would be what the UK government refers to as the state's social cohesion.<sup>[58]</sup> In several countries, this can be significantly undermined by using information supplied over IT means to create or exacerbate existing cleavages within societies or to incite anti-government groups who then drive disorder. This is what Russian military doctrine refers to as making use of the "protest potential of the population."<sup>[59]</sup> This potential may be seen as perhaps the Russian military's *most potent strategic weapon* in the near-term future against NATO states.

A large body of literature in Russia is devoted to describing how to incite this protest potential or how to make a population turn against its government. This form of warfare has been variously labeled by Russian authors such as Barthosh,<sup>[60]</sup> Evgenii Messner,<sup>[61]</sup> Andrei Kokoshin<sup>[62]</sup> and Valerii Konyshev and Aleksandr Sergunin – as "mental warfare," "rebellion wars," "wars of consciousness," and "political warfare."<sup>[63]</sup>

Today there is much more fertile ground than ever before for creating social cleavages across the Western world. This is especially so given the prevalence of social media, which often drives divisive populism and general societal discord. Indeed, both the US<sup>[64]</sup> and the UK<sup>[65]</sup> have blamed Russian misinformation/disinformation for stoking unrest within their respective countries. And some inkling of the type of disruption that Russian cyber-psychological operations would hope to generate (or perhaps have generated) could be seen with the storming of the US Capitol Building on January 6, 2021.<sup>[66]</sup> Such instances can only encourage the Russian military to increase the degree, tempo, and potency of its cyber-psychological operations in the future. This is particularly so as worldwide inflation begins to bite and social discontent rises in the Western world. Of course, NATO as a collective and its cohesion is a target here. Russia appears to be generating information-driven cleavages between member states to weaken the Alliance.<sup>[67]</sup>

According to Russian military logic, states that become so concerned with their internal security are ones that then tend to lose interest in their external security. They will look inwards to threats, not outwards.<sup>[68]</sup> When applied to NATO states, the benefits to Russia are obvious. Taking any momentous decisions regarding Russia by core NATO states or the Alliance itself would be difficult to generate if they had to concentrate on domestic problems. One result might be no threat to Russia of a consensus-reliant NATO decision being made to stand up to Russian aggression on the international stage or even, with perhaps Ukraine in mind, to engage in any kinetic action against Russia itself.

And then, of course, there is also the ultimate aim of Russian offensive cyber-psychological operations. If the protest potential can be tapped into with sufficient energy and if the degree of internal *khaos* (to use a Russian word employed by some analysts) created reaches a sufficient

pitch, then this may render a state ungovernable.<sup>[69]</sup> Such a collapse of the targeted state would equate, in Russian eyes, to its neutralization, its defeat.<sup>[70]</sup>

### *Cyber-technical operations*

In Russia's military playbook, cyber-technical operations, when used as a strategic tool against adversary states, have a different focus depending on the strategic situation.<sup>[71]</sup> In the current era of competition between NATO and Russia, they will not focus their cyber-technical activities on creating significant disruption or damage within the cyberspace and IT systems of NATO states. That is not to say that there have been no such attacks. There was, of course, the very damaging attack against Estonia in 2007, but this was related to a specific issue and was not part of some overall Russian campaign.<sup>[72]</sup> There have also been major Russian cyberattacks against (non-NATO) Ukraine in recent years that were seriously disruptive, even before the current war.<sup>[73]</sup> There have also been attacks against NATO countries that may be seen as clumsy and of no more than nuisance value in a strategic sense, including ransomware attacks.<sup>[74]</sup> There have also been attacks on electoral processes in Western countries with a cyber-technical element to them.<sup>[75]</sup>

From a strategic point of view, one can understand why current Russian cyber-technical activity would not aim to inflict major disruption within NATO states. Such acts carried out in an era of competition would serve no real strategic purpose. They would only create unnecessary diplomatic angst and might, however deniable, invite retaliation (including in the kinetic realm).<sup>[76]</sup>

Thus, while concerning to NATO states, Russian cyber-technical attacks currently cannot be seen as significant (see below regarding the Ukraine conflict). But a clear Russian game plan is apparent: such attacks can be seen largely as intrusions aimed at preparation for future activities at the strategic level. This preparation involves work in three spheres. First, cyber espionage will focus on stealing intellectual property and accessing secret information that could be useful to Russia's military and economy. The second will be reconnaissance; that is, looking for weaknesses in NATO countries' computer systems—both civil and military—that could be taken advantage of later. A third will be the clandestine planting of destructive malware in either military or CNI systems which can be triggered as part of a future “zero-day”<sup>h</sup> attack.<sup>[77]</sup>

The Russian aim seems obvious. Such *sub rosa* cyber-technical activities would all be designed for use during a state of actual armed hostilities with NATO or at times of high geopolitical tension when Russia no longer sees any reason for cyber warfare restraint. The hoped-for effects of a major cyber-technical assault would include:

- ◆ Turning off lights and power.
- ◆ Disabling industrial control systems.
- ◆ Crippling banking systems.
- ◆ Disrupting logistics chains (including food supplies).

<sup>h</sup> These are exploits of vulnerabilities in software not known to anyone but the hackers themselves. These exploits can be leveraged at any time (if undetected and not fixed), thereby creating a so-called “zero-day attack.”

The ideal Russian outcome would be that societies could no longer function; governments would lose control, and *khaos* could be induced again. It could all be achieved within a few hours. Russia imagines that the effect of such a catastrophically damaging cyberattack would be equivalent to that of an attack by nuclear weapons.<sup>[78]</sup> Here is the cherished goal of all Russian military operations: the *udar*—the crushing, mortal blow that is delivered with speed, surprise, and force. It would be at the strategic level and generated by non-kinetic and highly cost-effective cyberattacks that could theoretically be deniable.

With this bigger prize—the *udar*—in mind and given that this concept relies for effect ultimately on surprise, it should be expected that, in the immediate future, majorly disruptive Russian cyber-technical attacks will, where NATO states are concerned, not be apparent. The attacks that occur will remain limited in scope and largely confined to the aforementioned three spheres. In preparing for an *udar*, the Russian military will not want to show its cyber hand. It values cyber shock, not cyber attrition. But it can be surmised that the preparatory work: the espionage, reconnaissance and the planting of malware will, in the coming years, only be increasing in intensity so that the eventual cyber *udar* can be made as effective as possible (see also below).

### ***The power of offensive cyber***

Of course, the two forms of cyberattack—cyber-psychological and cyber-technical—can be used together: a gradual weakening process brought about by the former can be exacerbated by a later cyber-*blitzkrieg* application of the latter. Perhaps most concerning of all, though, for NATO states is that there will be a Russian determination to integrate artificial intelligence (AI) into its offensive cyber activities in the future. AI-enhanced cyber tools underpinned by powerful machine learning will open up new possibilities in both the cyber-psychological and cyber-technical realms.<sup>[79]</sup> In the former, disinformation campaigns could become much broader in scope and more focused in their targeting due to the power of algorithms and automation. In the technical realm, AI could offer, in Russian eyes, dramatic advantages. Indeed, the combination of AI and cyber could mean, as one advisor to the Russian military believes, that the Third World War might actually be over within just “a few seconds if one state takes control of all the main [cyber] life-support systems of rival countries using AI technology.”<sup>[80]</sup>

### ***The War in Ukraine***

Prior to Russia’s invasion of Ukraine there was obviously much hype about the quality of the offensive cyber capabilities that the Russian military could bring to bear.<sup>[81]</sup> Ukraine and, indeed, several NATO states were prepared for a major cyber onslaught by what was considered to be the “the most aggressive cyber actor in the world.”<sup>[82]</sup> But while there appears to have been many attempted attacks against Ukrainian targets their actual effectiveness has been judged to be limited (as of June 2022).<sup>[83]</sup> A Microsoft report in late June 2022 pointed to the fact that only 29 per cent of cyber-attacks on IT systems in Ukraine, the US, Poland, and the

Baltic States “breached the targeted networks.”<sup>[84]</sup> Either the attacks were thwarted or there appears to have been enough redundancy available to work around attacks that did reach their targets.<sup>[85]</sup> One possible reason for this lack of success is the fact that Ukraine’s cyber defenses had been bolstered, both before and during the conflict, by Western state actors and private corporations, including Microsoft and Elon Musk’s Starlink.<sup>[86]</sup>

There has also been little evidence of the use of AI-enhanced systems designed to generate cyber-psychological effects—such as the use of deepfakes (both video and voice)<sup>[87]</sup> and misinformation-spreading bots.<sup>[88]</sup> Moreover, the deepfake generated of Ukrainian President Volodymyr Zelensky at the beginning of the war, where he was ‘seen’ purportedly asking his troops to surrender, was not professionally produced. The next deepfake might, though, not be as easy to identify.<sup>[89]</sup>

However amateurish the deepfakes, the Microsoft report also noted that Russian offensive cyber seems to have been more effective in the cyber-psychological realm than in the cyber-technical. The spread of pro-Russian and anti-Ukrainian misinformation and disinformation across not just Ukraine but also the world at large is seen by this report to be a Russian success.<sup>[90]</sup> What was also noticeable was the coordination at times between cyber-technical and cyber-psychological attacks and actual kinetic strikes, which were designed to generate significant strategic effect.<sup>[91]</sup> This coordination was observed on several occasions, most notably when Russian missiles struck Kyiv’s TV tower on March 1, 2022. Several cyber-attacks accompanied the strike on Ukraine’s media companies. This combination of the use of offensive cyber and kinetic effect has been viewed as a multi-domain operation designed to have the strategic effect of generating chaos.<sup>[92]</sup> Also apparent has been the degree of Russian cyber espionage activity, especially against US systems. In this case, the help that Washington is providing to Ukraine in terms of cyber defense can only open Russian eyes to US cyber capabilities.<sup>[93]</sup>

But questions need to be asked about the employment of Russian offensive cyber when it comes to the Ukraine war. Why was it less apparent if the Russian military emphasized it before the conflict? Here it could be argued that there was a degree of underestimation of the target and a degree of hubris where its cyber capabilities were concerned.

There may, however, be other, more significant, issues at play. Admiral (Ret.) James Stavridis, the former Supreme Allied Commander of NATO forces, is wary of judging Russian offensive cyber based on the experience so far in Ukraine. He has noted that “Putin [is] saving massive scale non-deniable cyber-attacks for a later stage of the conflict.” He says this would be in retaliation for when Western “sanctions really start to bite.”<sup>[94]</sup> Another reason for the shortfall in effective cyber-technical interventions may be the Russian military not wanting to show its cyber hand. It is holding back on its true capabilities because of a concern over any future conflict with NATO itself. If such a conflict broke out, the military would want to create the aforementioned cyber *удар*. This shocking blow could render an immediate and overwhelming

effect on neutralizing adversary states. This shock value would be lost if NATO cyber defense specialists became aware of what Russian offensive cyber in the cyber-technical realm could do. These specialists could see where NATO's own vulnerabilities might lie and then take the necessary defensive action. NATO would be forewarned, and therefore, forearmed. Hence, the use of Russian offensive cyber as part of the Ukraine conflict may be limited because of the bigger strategic picture.<sup>[95]</sup> The Russian military might not want to waste perhaps the most effective weapon in its armory in the Ukraine conflict.

Thus, any analysis of the use of offensive cyber by the Russian military regarding the Ukraine conflict may not simply be a case of concluding that they are not as good as previously thought. It may not be as straightforward as this. There could be several rationales behind the lack of offensive cyber activities.

## CONCLUSION

Russia's military hierarchy and its political leaders see their country as facing an existential threat from NATO and being geopolitically constrained by NATO power. The military has thus, for several years now, been on what amounts to a (albeit non-kinetic) war footing with core NATO states. The aim is to neutralize: to weaken NATO and its core states from within, and specifically to undermine their resolve to take any collective action against Russia. Offensive cyber is a crucial weapon in this war.

The predominant variant of offensive cyber used thus far has been the cyber-psychological: the long-term application of misinformation and disinformation to shape political opinions and to break the bonds of social cohesion. The cyber-technical form is also being used. There has been a continued Russian campaign involving cyber-espionage, reconnaissance, and the planting of malware. And, if international tensions do rise significantly, the Russian military—and making use of this preparatory work—may then engage in a series of massive cyberattacks designed to target the IT systems of NATO states. Again, after being subject to such an attack, these states might be in no position – or have the willingness – to take collective action against Russia.

In essence, offensive cyber offers the Russian military the chance to impose Russian will on its NATO adversary. It appears to have no other tool available in its armory that could do this. But just how effective can this offensive cyber option actually be? The experience of Ukraine would say that there may be little substance here, that the threat has been exaggerated. It is difficult, though, to draw too many conclusions from what has happened in Ukraine so far. The Russian military's offensive cyber capabilities, in cyber-psychological and cyber-technical forms, may yet prove to be very effective. Each does hold the promise of neutralizing NATO adversaries without necessarily inciting kinetic conflict. Beyond what is happening in Ukraine, Russian offensive cyber must be recognized as a latent and growing threat to NATO and its core states.♥

## NOTES

1. United Kingdom Ministry of Defence. *Defence in a Competitive Age*. CP 411, March 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/974661/CP411\\_-\\_Defence\\_Command\\_Plan.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-_Defence_Command_Plan.pdf).
2. Janis Berzins, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies* 33, no 3 (2020): 355-80. DOI <https://doi.org/10.1080/13518046.2020.1824109>.
3. Elena Larina & Vladimir Ovchinskii, *Chas Volka: Vvedeniye v Khronopolitiku* [The Hour of the Wolf: Introduction to Chronopolitics] (Moscow: Knizhnyi Mir, 2019).
4. William Baxter, *Soviet Airland Battle Tactics* (Novato, CA: Presidio 1986), 10.
5. Simon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (London: Frank Cass, 1997), 172.
6. Konstantin Sivkov, "Pravo na Udar: Tol'ko Takaya Forma Vozdeystviya na Agressora Sorvet Ego Vozmozhnoye Voyennoye Vtorzheniye [A Right to Udar: Only Such a Form of Impact on the Aggressor Will Thwart his Possible Military Invasion]." VPK. Last modified March 3, 2014, <https://vpk-news.ru/articles/19370>.
7. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Anchor Books, 2020).
8. Andrei Soldatov & Irina Borogan, "The Man Behind Putin's Military," *Foreign Affairs*. Last modified February 26, 2022, <https://www.foreignaffairs.com/articles/2022-02-26/man-behind-putins-military>.
9. See Stephen Blank, "Cyber War and Information War a la Russe," in G. Perkovich and A. E. Levite (eds), *Understanding Cyber Conflict: Fourteen Analogies* (Washington DC: Georgetown University Press, 2017), 81-98; Jolanta Darczewska. "Russia's Armed Forces on the Information War Front," *OSW Studies*, no 57 (2016), [https://www.osw.waw.pl/sites/default/files/prace\\_57\\_ang\\_russias\\_armed\\_forces\\_net.pdf](https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf); Greenberg, *Sandworm*; Scott Jasper, *Russian Cyber Operations* (Washington D.C.: Georgetown University Press, 2020); Bilyana Lilly & Joe Cheravitch. "The Past, Present and Future of Russia's Cyber Strategy and Forces," in T. Jancarkova, L. Lindstrom, M. Signoretti and I. Tolga (eds), *20/20 Vision: The Next Decade* (Tallinn: NATO, 2020), [https://ccdcoc.org/uploads/2020/05/CyCon\\_2020\\_8\\_Lilly\\_Cheravitch.pdf](https://ccdcoc.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf); Frederick Westerlund, "Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?" FOI Memo no. 3126. Stockholm: FOI Swedish Research Defense Agency, 2010.
10. Valerii Gerasimov, "Vektory Razvitiya VoЕННОi Strategii [Vectors of Military Strategy Development]," *Krasnaya Zvezda*, last modified March 4, 2019, <http://redstar.ru/vektory-razvitiya-voennoj-strategii/>.
11. S. Chekinov & S. Bogdanov, "O Kharaktere I Soderzhanii Voiny Novogo Pokoleniya [On the Character and Content of New-Generation Wars]," *Voennaya Mysl'* 22, no. 4 (2013): 13–24; A.V. Kartapolov, "Uroki Voennykh Konfliktov, Perspektivy Razvitiya Sredstv I Spocobov ikh Vedeniya. Pryamye I Nepryamye Deistviya v Sovremennykh Mezhdunarodnykh Konfliktov [Lessons of Military Conflicts and Prospects for the Development of Means and Methods for their Conduct. Direct and Indirect Actions in Contemporary International Conflicts]," *Vestnik Akademii Voennykh Nauk*, no. 2 (2015), <http://www.avnr.ru/index.php/zhurnal-qvoennyj-vestnikov/arkhiv-nomerov/737-vestnik-avn-2-2015>; "Putin: Rossiya Vynuzhdena Otvechat' na Sozdaniye Ugrozy na Territorii Ukrainy Silami NATO [Putin: Russia is Forced to Respond to the Creation of Threats on Ukraine's Territory by NATO Forces]," *Kommersant*, last modified January 31, 2021, <https://www.kommersant.ru/doc/5100337>; Stephanie Pezard and Ashley L. Rhoades, *What Provokes Putin's Russia? Deterring Without Unintended Escalation* (Santa Monica, CA: RAND Corporation, 2020), <https://www.rand.org/pubs/perspectives/PE338.html>; "Putin's Munich Speech 15 Years Later: What Prophecies Have Come True?" TASS, last modified February 10, 2022, <https://tass.com/politics/1401215>.
12. Valerii Gerasimov, "NATO Ne Prigovor [NATO is not a Sentence]," *Voенно-Promyshlennyi Kur'er*, last modified April 30, 2019, <https://vpk-news.ru/articles/49970>; Kartapolov, "Lessons of Military Conflicts"; A.A. Kokoshin, *Voprosy Prikladnoi Teorii Voyny* [Questions of Applied Theory of War] (Moscow: Izdatels'kiy Dom VSHE, 2019); "Putin: Russia is Forced," *Kommersant*, 2021; V.N. Konyshov & A. Sergunin, *Sovremennaya Voennaya Strategiya* [Modern Military Strategy] (Moscow: Aspekt Press, 2014).
13. Ministry of Defense of the Russian Federation, *Voennaya Doktrina Rossiiskoi Federatsii* [Military Doctrine of the Russian Federation], Kremlin, last modified December 26, 2014, <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>.
14. Ministry of Defense of the Russian Federation, *Strategiya natsionalnoi bezopasnosti Rossiiskoi Federatsii* [National Security Strategy of the Russian Federation], Website of the Russian Security Council, last modified July 2, 2021, <http://scr.f.gov.ru/security/docs/document133/>.

## NOTES

15. Chekinov & Bogdanov, "On the Character and Content of New-Generation Wars"; Kartapolov, "Lessons of Military Conflicts"; Valerii Gerasimov, "Genshtab Planiruyet Udary [The General Staff Plans Strikes]," *Voенно-Promyshlennyy Kur'er* 9, no. 772, last modified March 12, 2019, <https://vpk-news.ru/articles/48913>; "Putin's Munich Speech 15 Years Later" TASS, 2022.
16. Chekinov & Bogdanov, "On the Character and Content of New-Generation Wars"; Kartapolov, "Lessons of Military Conflicts"; Richard Sokolsky, "The New NATO-Russia Military Balance: Implications for European Security," *Carnegie Endowment*, last modified March 13, 2017, <https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222>.
17. Bryan Frederick, Matthew Povlock, Stephen Watts, Miranda Priebe & Edward Geist, *Assessing Russia's Reactions to U.S. and NATO Posture Enhancements* (Santa Monica, CA: RAND Corporation, 2017), [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1800/RR1879/RAND\\_RR1879.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1879/RAND_RR1879.pdf).
18. A.E. Sterlin & A.L. Khryapin, "Ob Osnovakh Gosudarstvennoy Politiki Rossiiskoi Federatsii v Oblasti Yadernogo Sderzhivaniya [On Foundations of Government Policy of the Russian Federation in Sphere of Nuclear Containment]," *Krasnaya Zvezda*, last modified August 7, 2020, <http://redstar.ru/ob-osnovah-gosudarstvennoj-politiki-rossijskoj-federatsii-v-oblasti-yadernogo-sderzhivaniya>; "Putin Rasskazal o 'Pervom Udare' I Vozmozhnosti Primeneniya Yadernogo Oruzhiya Rossiyei [Putin Spoke about the 'First Strike' and the Possibility of Using Nuclear Weapons by Russia]," *Sputnik Latvia*, last modified December 11, 2020, <https://lv.sputniknews.ru/20201111/Putin-rasskazal-o-pervom-udare-i-vozmozhnosti-primeneniya-yadernogo-oruzhiya-Rossiey-14656937.html>.
19. Gerasimov, "The General Staff Plans Strikes."
20. Rod Thornton, "Countering Prompt Global Strike: The Russian Military Presence in Syria and the Eastern Mediterranean and Its Strategic Deterrence Role," *Journal of Slavic Military Studies* 31, no. 1 (2019): 1-24, <https://doi.org/10.1080/13518046.2019.1552655>; "V Genshtabe Sochli Tselyu Kontseptsii SSHA 'Global'nyi Udar' Dominirovaniye v Mire [The General Staff considered the Goal of the US Concept 'Global Strike' to Be the Dominance of the World]," *Interfax*. Last modified Aug 7, 2020, <https://www.interfax.ru/russia/720674>; "Ugroza Global'nogo Udara SSHA Yavlyayetsya Osnovoi dlya Rossiiskoi VKO [The Threat of a US Global Strike Forms a Basis for Russian Air Space Defense]," *RIA Novosti*. Last modified April 4, 2015, <https://ria.ru/20150404/1056636168.html>.
21. Yakov Kedmi, "Moscow on the Euphrates," *Israel Defence*, No. 40 (Winter 2018).
22. Gerasimov, "The General Staff Plans Strikes"; Lyudmila V. Gundarova, "Kto Finansiruyet Tsvetnyye Revolyutsii na Postsovetskom Prostranstve [Who Finances Color Revolutions in the post-Soviet Space]," *Nezavisimoe Voенnoe Obozrenie*. Last modified Jan 15, 2016, [https://nvo.ng.ru/concepts/2016-01-15/1\\_revolutions.html](https://nvo.ng.ru/concepts/2016-01-15/1_revolutions.html); "S 'Tsvetnykh Revolyutsiy' Hotyat Snyat' Kamuflyazh [They Want to Remove Camouflage from 'Color Revolutions']," *Kommersant*. Last modified April 3, 2015, <https://www.kommersant.ru/doc/2679357>; "Rossiya Obvinila NATO v Podgotovke 'Tsvetnykh Revolyutsiy' [Russia Blamed NATO for Preparing 'Color Revolutions']," *Lenta*. Last modified July 2, 2019, <https://lenta.ru/news/2019/07/02/sovbez/>.
23. V.N. Konyshchev & R.V. Parfenov, "Gibridnye Voyny: Mezhdru Mifom y Real'nostryu [Hybrid Wars: Between Myths and Reality]," *Mirovaya Ekonomika y Mezhdunarodnyye Otnosheniya*, no. 12 (2019): 56-66. <http://liber.hse.perm.ru/absopac/app/webroot/index.php?url=/notices/index/IdNotice:93892/Source:default; MoD RF, Military Doctrine of the Russian Federation 2014>.
24. (Col.) S. Chekinov & Lt-Gen. S. Bogdanov, "Asimmetrichnie deystviya po obespecheniyu voennoy bezopasnosti Rossii [Ensuring Russian military security by asymmetric means]," *Voennaya mysl'* no. 3 (2010): 13-22; (Col.) S. Chekinov & Lt-Gen. S. Bogdanov, "Vliyaniye Nepryamykh Deystviy na Kharakter Sovremennoy Voyny [The impact of indirect methods on the nature of modern warfare]," *Voennaya mysl'* no. 6 (2011): 3-13; Chekinov & Bogdanov. "On the Character," 16-18; Kartapolov, "Lessons of Military Conflicts."

NOTES

25. Andrew Fatter, “Dialog o Strategicheskoi Stabil’nosti [Dialogue about Strategic Stability],” *Valdai Club*, last modified September 1, 2021, <https://ru.valdaiclub.com/a/highlights/dialog-o-strategicheskoy-stabilnosti/>; “Putin Nazval Dolyu Sovremennogo Yadernogo Oruzhiya [Putin named the fate of contemporary nuclear weapons],” *Regnum*, last modified August 23, 2021, <https://regnum.ru/news/economy/3350979.html>; “Oruzhiye Rossii: O Chem Putin Govoril v Poslanii Sovfedu [Russia’s Weapons: What Putin spoke about in his message to the Federation Council],” *Ria Novosti*. Last modified April 22, 2021, <https://crimea.ria.ru/20210422/Oruzhie-Putina-o-chem-prezident-govoril-v-poslanii-Sovfedu-1119496017.html>; Markell Boystov, “Strategicheskaya Stabil’nost’, Zderzhivanniye Ustrasheniye I Yadernyi Simbioz [Strategic Stability, Containment through Deterrence, and Nuclear Symbiosis],” *Nezavisimoye Voennoye Obozreniye*. Last modified September 2, 2021, [https://nvo.ng.ru/armament/2021-09-02/1\\_1156\\_stability.html](https://nvo.ng.ru/armament/2021-09-02/1_1156_stability.html); “Rossiyane Polyubili Atomnuyu Bomby [Russians Learned to Love the Atomic Bomb],” *Vedomosti*. Last modified September 13, 2021, <https://www.vedomosti.ru/society/articles/2021/09/13/886490-rossiyane-bombu>.
26. Keir Giles & Mathieu Boulegue, “Russia’s A2/AD Capabilities: Real and Imagined,” *Parameters* 49, no. 1 (2019): 21-36. <https://press.armywarcollege.edu/parameters/vol49/iss1/4/>.
27. “NI: S-500 Obezpechit Pritsipa! no Novyi Uroven’ Zashchity [NI: S-500 will Provide a Fundamentally Different Level of Protection],” *RG*. Last modified August 2, 2021, <https://rg.ru/2021/02/08/ni-s-500-obezpechit-principialno-novj-uroven-zashchity.html>.
28. United States Army, *The US Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1, 2018, <https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf>.
29. Yaacov Falkov, “Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach,” *Intelligence and National Security* 37, no. 1 (2022): 90-108, <https://doi.org/10.1080/02684527.2021.1978135>.
30. Maj.-Gen. A. V. Serzhantov, “Transformatsiya Soderzhaniya Voiny: Ot Proshlogo k Sovremennomu [Transformation of the Concept of War: From Past to Present],” *Voennaya Mysl’*, no 1 (2021), 58.
31. Gerasimov, “Vectors of Military Strategy”; Gerasimov, “The General Staff Plans Strikes.”
32. Blank, “Cyber War and Information War a la Russe”; Sivkov, “A Right to Udar;” Rory Cormac & Richard Aldrich, “Grey is the New Black: Covert Action and Implausible Deniability,” *International Affairs* 94, no. 3 (2018), [https://warwick.ac.uk/fac/soc/pais/people/aldrich/secrets/inta94\\_3\\_01\\_cormac\\_aldrich.published.pdf](https://warwick.ac.uk/fac/soc/pais/people/aldrich/secrets/inta94_3_01_cormac_aldrich.published.pdf).
33. Gerasimov, “Vectors of Military Strategy.”
34. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020); A. Doronin, “Aktivnye Meropriyatiya: Informacionno-Psikhologicheskoe Vozdeistviye [Active Measures: Informational-psychological Influence],” *Agentura*. Last modified n.d. <https://www.agentura.ru/equipment/psih/info/activ/>; Maren Garberg Bredeesen & Karsten Friis, “Missiles, Vessels and Active Defence,” *The RUSI Journal* 165, no. 5-6 (2020): 68-78, <https://doi.org/10.1080/03071847.2020.1829991>; Dmitry (Dima) Adamsky, “From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture,” *Journal of Strategic Studies* 41, no. 1-2 (2018): 33-60, <https://doi.org/10.1080/01402390.2017.1347872>.
35. Gerasimov, “The General Staff Plans Strikes.”
36. Rod Thornton & Marina Miron, “The Role of Aktivnost’ Today in Russian Military-strategic Thinking and the Crucial Target of the ‘Protest Potential of the Population,’” in *Russian Concept of Deterrence in Contemporary and Classic Perspective*, ed. Pentti Forsström (National Defence University, Department of Warfare, Series 2: Research Reports No. 11, 2021).
37. Doronin, “Active Measures.”
38. Pavel Felgenhauer, “Dobitsya Prevokhodstva nad Ostol’nym Chelovechestvom [Achieving Superiority over the Rest of Humanity],” *Novaya Gazeta*. Last modified March 19, 2019, <https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom>.
39. Valerii Gerasimov, “Zennost’ Nauki v Predvidenii [The Value of Science in Foresight],” *Voенно-Promyshlennyi Kur’er*, last modified February 26, 2013, <https://vpk-news.ru/articles/14632>.
40. Felgenhauer, “Achieving Superiority over the Rest of Humanity.”
41. (Maj.) Yevgenii V. Safaryan, “Voennye Vyzovy I Ugrozy Dlya Rossiiskoi Federatsii (Na Period 2030-2040 Godov) [Military Challenges and Threats to the Russian Federation: 2030-2040],” *Voennaya Mysl’*, no. 4 (2021): 14-19.
42. Gerasimov, “Vectors of Military Strategy”; Gerasimov, “The General Staff Plans Strikes”; Thornton & Miron, “The Role of Aktivnost’”; Safaryan, “Military Challenges and Threats”; Serzhantov, “Transformation of the Concept of War.”
43. Gerasimov, “Vectors of Military Strategy.”

## NOTES

44. V. M. Baryn'kin, "Minnoe Pole Informatsionnykh Voin [The Minefield of Information Wars]," *Voenna-Promyshlennii Kur'er* [Military-Industrial Courier], no. 14 (2013); Chekinov & Bogdanov, "Ensuring Russian Military Security"; Chekinov & Bogdanov, "The Impact of Indirect Methods"; Gerasimov, "The General Staff Plans Strikes"; Konyshev & Sergunin, *Modern Military Strategy*; S. P. Rastorguyev, "Information Warfare as a Purposeful Information Impact of Information Systems," *Information Society*, Vol. 1 (1997). <http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/5c8e75b6b46dfd0dc32575be00396796>; S. P. Rastorguyev, *Formula Informatsionnoi Voyny* [Formula of Information War] (Moscow: Biblioteka Rasvoi Mysli, 1999).
45. Joseph S. Gordon, *Psychological Operations: The Soviet Challenge* (New York: Routledge, 1988).
46. Chekinov & Bogdanov, "On the Character"; Kartapolov, "Lessons of Military Conflicts"; Joe Gould and Mark Pomerleau, "Why the US Should Fight Russia, China in the 'Gray Zone'," *C4ISRNET*, last modified January 4, 2022, <https://www.c4isrnet.com/information-warfare/2022/01/04/why-the-us-should-fight-russia-china-in-the-gray-zone/>; Safaryan, "Military Challenges"; Clementine Starling, Tyson, Wetzel & Christian Trotti, "Seizing the Advantage: A Vision for the Next US Defense Strategy," Atlantic Council, last modified December 22, 2022, <https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/seizing-the-advantage-a-vision-for-the-next-us-national-defense-strategy/>.
47. Joan Prats I Amoros & Augustin Guillaume Barry, "Not Only Blood. The Need to Integrate Psychological Operations into the West's Military Culture," *Instituto Español de Estudios Estratégicos*, last modified September 19, 2019, [https://www.iese.es/Galerias/fichero/docs\\_opinion/2019/DIEEE81\\_2019JOAPRA\\_Psyops\\_ENG.pdf](https://www.iese.es/Galerias/fichero/docs_opinion/2019/DIEEE81_2019JOAPRA_Psyops_ENG.pdf); Ivana Stradner, "The US Must Turn the Tables on Russia's Psyops," *Defense One*, last modified November 17, 2021, <https://www.defenseone.com/ideas/2021/11/us-must-turn-tables-russias-psyops/186906/>; Kier Giles, "The Next Phase of Russian Information Warfare," *NATO Strategic Communications Centre of Excellence*, last modified May 20, 2016, <https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176>.
48. D. V. Galkin, P. A. Kolyandra & A. V. Stepanov, "Sostoyaniye I Perspektivy Ispol'zovaniya Iskysstvennogo Intellekta v Voennom Dele [Status and Prospects of Using Artificial Intelligence in Military Affairs]," *Voennaya Mysl'*, no 1 (2021): 113-124.
49. A.A. Barthosh, "Gibridnaya, Skrytnaya, Nepredskazuyemaya [Hybrid, Covert, Unpredictable]," *Nezavisimoye Voennoye Obozreniye*. Last modified August 12, 2021, [https://nvo.ng.ru/gpolit/2021-08-12/1\\_10\\_11\\_1153\\_hybrid.html](https://nvo.ng.ru/gpolit/2021-08-12/1_10_11_1153_hybrid.html).
50. Lilly & Cheravitch, "The Past, Present and Future."
51. Ibid.
52. Chekinov & Bogdanov, "On the Character"; Kartapolov, "Lessons of Military Conflicts"; Aleksandr Losev, "Voennii Iskusstvenii Intellect [Military Artificial Intelligence]," *Arsenal Otechestva* 6, no. 32 (January 2018), <http://arsenal-otechestva.ru/article/990-voennyj-iskusstvennyj-intellekt>.
53. A.A. Barthosh, "Model Gibridnoi Voyny [The Model of Hybrid Warfare]," *Voennaya Mysl'*, Last modified May 1, 2019, <https://vm.ric.mil.ru/Stati/item/191517>; Chekinov & Bogdanov, "On the Character"; Valerii Gerasimov, "Mir Na Grane Voyny [The World on the Brink of War]," *Voenna-Promyshlennyi Kur'er* 10, no. 674, last modified March 15, 2017, <https://vpk-news.ru/articles/35591>; Gerasimov, "The General Staff Plans Strikes"; I. Panarin, SMI, *Propaganda I Informacionnyye Voyny* [Media, Propaganda and Information Wars] (Moscow: Pokolenie, 2012); I. N. Vorobyov & V. A. Kiselyov, "Kiberprostranstvo kak sfera nepryamogo vooruzhennogo protivoborstva [Cyberspace as a sphere of indirect armed conflict]," *Voennaya Mysl'*, no. 12 (2014): 21-28.
54. Jasper, Russian Cyber Operations.
55. BBC Monitoring, "Russian Foreign Intelligence Chief Accuses West of 'Destructive interference,'" *BBC Monitoring*, last modified October 13, 2021, <https://monitoring.bbc.co.uk/product/c202yc9o>.
56. Vladimir A. Lefebvre, *Konfliktuyushhiye Struktury* [Conflicting Structures] (Moscow: Vysshaya Shkola, 1967); Vladimir A. Lefebvre, *Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process* (Moscow: Science Applications, 1984); Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no 2 (2004): 237-256, <https://doi.org/10.1080/13518040490450529>.

## NOTES

57. Lauriens Cerulus, “France Identifies Russia-linked Hackers in Large Cyberattack,” *Politico*. Last modified February 15, 2021, <https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/>; Andreas Rinke & Kristi Knolle, “Russia Responsible for Cyber Attacks on German Parliament – German Foreign Ministry,” *Reuters*. Last modified September 6, 2021, <https://www.reuters.com/world/europe/russia-responsible-cyber-attacks-german-parliament-german-foreign-ministry-2021-09-06/>; Christopher Bing, Joseph Menn & Raphael Satter, “Putin Likely Directed 2020 U.S. Election Meddling, U.S. Intelligence Finds,” *Reuters*. Last modified March 16, 2021, [https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1635621136580](https://www.reuters.com/article/usa-election-cyber-int-idUSKBN2B82PF; Dina Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story of The SolarWinds Hack,” <i>NPR</i>, last modified April 16, 2021, <a href=).
58. United Kingdom Ministry of Defence, “Defence in a Competitive Age.”
59. Ministry of Defence of the Russian Federation, *Military Doctrine*.
60. A.A. Barthosh, “Strategiya I Kontrastrategiya Gibridoi Voyny [Strategy and Counterstrategy of Hybrid War],” *Voennaya Mysl*, no. 10 (2018): 5–19.
61. Evgenii Messner, *Khochesh’ Mira, Pobedi Myatezhvoynu* [If You Want Peace, Win the Rebellion War] (Moscow: Military University Russkii Put’, 2005).
62. Kokoshin, *Questions of Applied Theory of War*.
63. Konyshov & Sergunin, *Modern Military Strategy*.
64. Julian Barnes & Adam Goldman, “Russian Trying to Stoke Racial Tensions Before Election, Officials Say,” *The New York Times*, last modified March 16, 2021, <https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html>.
65. United Kingdom Intelligence and Security Committee, Russia Report (Intelligence and Security Committee of Parliament, 2020), [https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207\\_CCS0221966010-001\\_Russia-Report-v02-Web\\_Accessible.pdf](https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf).
66. Julian Borger, “When White Supremacist came to the US Capitol,” *The Guardian*, last modified January 9, 2021, <https://www.theguardian.com/us-news/2021/jan/09/us-capitol-insurrection-white-supremacist-terror>; Ronald F. Inglehart, & Pippa Norris, “Trump, Brexit and the Rise of Populism; Economic Have-nots and Cultural Backlash,” *Harvard Kennedy School Working Paper* (2016), [https://formiche.net/wp-content/blogs.dir/10051/files/2017/01/RWP16-026\\_Norris.pdf](https://formiche.net/wp-content/blogs.dir/10051/files/2017/01/RWP16-026_Norris.pdf).
67. Geir Hagen Karlsen, “Divide and Rule: Ten Lessons About Russian Political Influence Activities in Europe,” *Humanities and Social Sciences Communications* (2019), <https://www.nature.com/articles/s41599-019-0227-8>.
68. Chekinov & Bogadnov, “Ensuring Russian military security”; Chekinov & Bogadnov, “The Impact of Indirect Methods”; Chekinov & Bogadnov, “On the Character;” Karatapolov, “Lessons of Military Conflicts.”
69. Chekinov & Bogdanov, “On the Character.”
70. *Ibid.*; Kartapolov, “Lessons of Military Conflicts.”
71. Greenberg, *Sandworm*; Jasper, *Russian Cyber Operations*.
72. Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” *NATO CCDCOE*, last modified October 2018, [https://ccdcoe.org/uploads/2018/10/Ottis2008\\_AnalysisOf2007FromTheInformationWarfarePerspective.pdf](https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf).
73. Greenberg, *Sandworm*; Colin Demarest, “Blue, Yellow and Grey Zone: The Cyber Factor in Ukraine,” *C4ISRnet*, last modified March 14, 2022, <https://www.c4isrnet.com/cyber/2022/03/14/blue-yellow-and-gray-zone-the-cyber-factor-in-ukraine/>.
74. United Kingdom National Cyber Security Centre, “Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed,” *NCSC.gov*. Last modified October 3, 2018, <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>; United States Cybersecurity and Infrastructure Agency, “Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders,” *CISA.gov*, last modified April 26, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa21-116a>.
75. Heather Conley & Jean-Baptiste Jeangene Vilmer, “Successfully Countering Russian Electoral Interference,” *CSIS Briefs*, last modified June 21, 2018, <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference>.
76. Greenberg, *Sandworm*; Jasper, *Russian Cyber Operations*.

NOTES

77. “Russian Cyber Units,” *Congressional Research Service*, last modified February 2, 2022, <https://crsreports.congress.gov/product/pdf/IF/IF11718c>; Greenberg, Sandworm; Westerlund, “Russian Intelligence Gathering;” Josephine Wolff, “Understanding Russia’s Cyber Strategy,” *Foreign Policy Research Institute*, last modified July 6, 2021, <https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/>.
78. Larina & Ovchinskii, *The Hour of the Wolf*; “Kiberataki Strashnee, Chem Yadernoye Oruzhiye: Kak Mirovye SMI Otreagi-rovali na Virus Petya [Cyberattacks are Scarier than Nuclear Weapons: How the Global Media Reacted to the Petya Virus],” TASS, last modified June 29, 2017, <https://tass.ru/mezhdunarodnaya-panorama/4374732>.
79. Thornton & Miron, “The Role of Aktivnost”; Vasilii Kashin, “Vliyaniye Kiberoruzhiya na Strategicheskuyu Stabil’nost’ v XXI Veke [The Impact of Cyber Weapons on Strategic Stability in the 21st Century],” Carnegie Endowment for International Peace, last modified December 27, 2018, <https://carnegie.ru/commentary/78033>; Galkin, Kolyandra & Stepanov, “Status and Prospects of Using Artificial Intelligence;” D. V. Galkin & A.V. Stepanov, “Voprosy Bezopasnosti Primeneniya Iskusstvennogo Intellekta v Sistemakh Voennogo Naznacheniya [Security Questions of the Use of AI in Military Systems],” *Voennaya Mysl’*, no. 4 (2021): 72-79.
80. Losev, “Military Artificial Intelligence.”
81. Ryan Browne, “The world is bracing for a global cyberwar as Russia invades Ukraine,” CNBC, last modified February 25, 2022, <https://www.cnbc.com/2022/02/25/will-the-russia-ukraine-crisis-lead-to-a-global-cyber-war.html>.
82. Eric Tegler, “The vulnerability of AI systems may explain why Russia isn’t using them extensively in Ukraine,” *Forbes*, last modified March 16, 2022, <https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/?sh=5ecf559837d5>
83. Raphael Satter, Christopher Bing, and James Pearson, “Microsoft Discloses Onslaught of Russian Cyber Attacks on Ukraine,” *Reuters*, last modified April 27, 2022, <https://reuters.com/technology/microsoft-discloses-onslaught-russian-cyberattacks-ukraine-2022-04-27/>.
84. “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft, last modified June 22, 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>.
85. David E. Sangar & Julian Barnes, “Many Russian Cyber Attacks Failed in First Months of Ukraine War, Study Finds,” *The New York Times*, last modified June 22, 2022, <https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html>.
86. Christopher Miller, Mark Scott, and Bryan Bender, “UkraineX: How Elon Musk’s Space Satellites Changed the War on the Ground,” *Politico*, last modified June 8, 2022, <https://www.politico.eu/article/elon-musk-ukraine-starlink>.
87. Philip Oltermann, “European politicians duped into deepfake video calls with the mayor of Kyiv,” *The Guardian*, June 25, 2022, <https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko?amp;amp>.
88. Tegler, “The vulnerability of AI systems may explain why Russia isn’t using them extensively in Ukraine.”
89. Tom Simonite, “A Zelensky Deepfake Was Quickly Defeated. A Next One Might Not Be,” *WIRED*, last modified March 17, 2022, <https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/>.
90. “Defending Ukraine.”
91. Satter, Bing, and Pearson, “Microsoft Discloses.”
92. Danyil Martinyak, “‘Unprecedented’ Cyberattack Blamed on Russia Was Meant to Sow Chaos in Ukraine,” *Asia News*, last modified February 17, 2022, [https://central.asia-news.com/en\\_GB/articles/cnmi\\_ca/features/2022/02/17/feature-01](https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2022/02/17/feature-01); Clare Roth, “Ukraine Cyberwar Creates Chaos, ‘It Won’t Win the War,’” *Deutsche Welle*, last modified March 3, 2022, <https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197>.
93. Sean Lyngaas, “Microsoft Says Russia Has Stepped Up Cyber Espionage Against the US and Ukraine Allies,” CNN, last modified June 22, 2022, <https://edition.cnn.com/2022/06/22/politics/microsoft-russia-hackings/index.html>.
94. Catherine Philp, “Putin armed cyberattack aimed at me, says former MI6 chief,” *The Times*, last modified May 26, 2022, <https://www.thetimes.co.uk/article/putin-aimed-cyberattack-at-me-says-former-mi6-chief-sir-richard-dearlove-xtlq83cql>.
95. Jaspreet Gill, “Russia May Be Holding Cyber Capabilities In Reserve, So U.S. Must Keep Its Shields Up: Experts,” *Breaking Defence*, last modified March 14, 2022, <https://breakingdefense.com/2022/03/russia-may-be-holding-cyber-capabilities-in-reserve-so-us-must-keep-its-shields-up-experts/>.

---

---

# THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

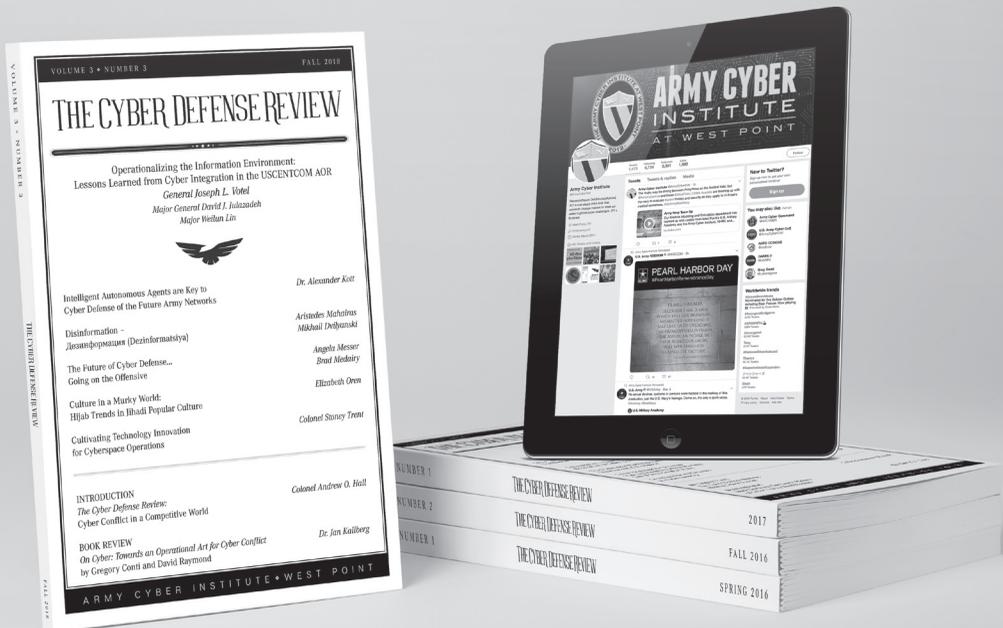
 [CyberDefenseReview.Army.mil](http://CyberDefenseReview.Army.mil)

AND THROUGH SOCIAL MEDIA

 Facebook [@ArmyCyberInstitute](https://www.facebook.com/ArmyCyberInstitute)

 LinkedIn [@LinkedInGroup](https://www.linkedin.com/company/ArmyCyberInstitute)

 Twitter [@ArmyCyberInst](https://twitter.com/ArmyCyberInst)  
[@CyberDefReview](https://twitter.com/CyberDefReview)



ARMY CYBER INSTITUTE ♦ WEST POINT PRESS





# WEST POINT PRESS



---

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.