Military Cyber Affairs

Volume 6
Issue 1 *HammerCon 2023 Issue*

Article 3

May 2023

What Senior U.S. Leaders Say We Should Know About Cyber

Dr. Joseph H. Schafer
National Defense University, College of Information and Cyberspace, joseph.schafer@milcyber.org

What Senior U.S. Leaders Say We Should Know About Cyber

Cover Page Footnote

I thank the Atlantic Council, particularly Kemba Walden, Jen Easterly, Nate Fick, and Marshall Miller, for helping advance this research.

What Senior U.S. Leaders Say We Should Know About Cyber

Dr. Joseph Hughes Schafer

Implementing the U.S. 2023 National Cybersecurity Strategy

On April 6, 2023, the Atlantic Council's Cyber Statecraft Initiative hosted a panel discussion on the new National Cybersecurity Strategy. The panel featured four senior officials from the Office of the National Cyber Director (ONCD), the Department of State (DoS), the Department of Justice (DoJ), and the Department of Homeland Security (DHS).[1] The author attended and asked each official to identify the most important elements that policymakers and strategists must understand about cyber. This article highlights historical and recent struggles to express cyber policy, the responses from these officials, and concludes with the author's ongoing research to improve national security cyber policy.

Released by President Biden on March 1, 2023, the new National Cybersecurity Strategy (NCS), reinforces themes from earlier strategies. It aspires to increase collaboration around five pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

The new NCS prominently aims to shift U.S. allocation of roles, responsibilities, and resources in cyberspace by, 1) Rebalancing the responsibility to defend cyberspace, and, 2) Realigning incentives to favor long-term investments. These shifts seek to strengthen defenses and alter the dynamics that continue to confound our interests (Biden 2023, 4–5).

[1] These officials were: Kemba Walden, Acting National Cyber Director, ONCD at the White House; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA) at DHS, Ambassador Nathaniel Fick, Ambassador at Large for Cyberspace and Digital Policy at DoS; and Marshall Miller, Principal Associate Deputy Attorney General at DoJ.

National Security Cyber-Attacks

Malign actors continue to confound our interests. The Center for Strategic and International Studies (CSIS), a prominent D.C. think-tank, documents *significant national security* cyber-attacks every week – a small but prominent subset of the thousands of cyber-attacks launched daily.[2] These powerful national security attacks include those damaging government agencies, defense companies, and critical infrastructure; and those causing losses exceeding one million dollars. Adversarial states and their clients are behind most of these attacks; however, U.S. national security leaders struggle to articulate sound cyber policy.[3]

An egregious example is a 1983 policy equating cyber with nuclear weapons, i.e. weapons of mass destruction (WMD), that stifled U.S. cyber activities for four decades (Kaplan 2017). The U.S. was not alone; Russia initiated cyber discussions in the United Nations (UN) twenty-five years ago (Korzak 2021, 5). Russia submitted a draft resolution explicitly equating nuclear / WMD with cyber information weapons "…the destructive 'effect' of which may be comparable to that of weapons of mass destruction" (Lavrov 1998, 2). Despite these policy stances, however, unlike nuclear conflict, which has not occurred since 1945, cyber conflict remains aggressive and continuous.

Historical Struggles: Cyber is not Nuclear

In June 1983, President Ronald Reagan screened the movie *WarGames* about a teen hacker who almost (accidentally) launches World War Three. Two days later, Reagan asked John Vessey, Chairman of the Joint Chiefs, "Could something like this really happen?" One week later, General Vessey returned with a startling answer, "Mr. President, the problem is much worse than you think" (Kaplan 2017). This resulted in the first presidential directive on computer security and represents the foundation of suboptimal U.S. cyber policies. These policies equated cyber deterrence with nuclear deterrence. They required presidential approval before the employment of U.S. cyber capabilities, stifling the maturation of cyber capacity, planning, and policy.

This false equivalence was carried into law enforcement when the FBI arrested renowned hacker, Kevin Mitnick, in 1995. He spent five years in prison (Soesanto and Smeets 2021) because the judge was convinced that Mitnick could initiate "a nuclear war by whistling on a public telephone" (Mitnick, Kevin, Simon, William L., and Wozniak, Steve 2012).

---

[2] Terminology varies. Cyber "attacks" may be "incidents" in national security contexts. (Bulao 2022) and (CSIS 2022). Similarly, interchangeable use of "cybersecurity" versus the broader "cyber" may blur concepts. E.g. DoD also maintains a public website on cyber*security* with the title "Cyber" (DoD 2022) and (DoD 2023).

[3] Elements in this article draw from the author's unpublished research. (Schafer 2023)

DOI: https://doi.org/10.5038/2378-0789.6.1.1089

The field continued to mature and from 2009 until 2012, NATO convened an international group of experts to document norms for cyberspace operations. They published the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013 (Schmitt 2013), documenting relevant legal regimes in the cyber context. The focus was on cyber power and warfare *armed attacks* which allow states to respond in self-defense, a provocation that arguably has not occurred. A second and more diverse group of experts published *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* in 2017, adding topics reflecting the reality of daily information power and cyberspace *operations* in peacetime that do not rise to the level of armed conflict (Schmitt 2017). Both manuals reflect *the law as it exists* according to international experts and describe the legal limits for operations in information and cyberspace (Jensen 2017, 738).

A continuing national security cyber challenge is that international norms in information and cyberspace remain unacknowledged by adversarial regimes. The strategic competition between great powers, other states, and proxies has increasingly been played out in cyberspace. National security leaders especially grapple with appreciating the continuous malign activities in this virtual domain and the implications of strategic competition among states and proxy actors (Schafer 2020). The inability to compete diplomatically, militarily (conventionally), or economically motivates aggressive state actors to continue to concentrate on cyber power operations and continue the great game in cyberspace.

Recent Military Emphasis on Cyberspace

Indeed, although the great game in cyberspace is increasingly played against the backdrop of great power competition, in many ways, cyber continues to be very technical and very siloed. Rather than focusing on the "bits and bytes", national security leaders must understand how cyber capabilities contribute to strategic and operational objectives and be able to ask the right questions and make decisions about how to integrate capabilities to achieve objectives (Leitzel and Hillebrand, Gregory D. 2022, 3). A foundational understanding of the breadth and depth cyberspace by leaders remains critical particularly as U.S. military emphasis on cyberspace has surged in the past few years with:

1. The recognition that Cyberspace is the fifth domain of warfare (alongside Land, Sea, Air, and Space) in the *2004 National Military Strategy* (DoD 2004)

2. The promotion of the U.S. Cyber Command to Combatant Command status (USCYBERCOM) in 2010, the activation of the Cyber Mission Force (CMF) in 2012, (USCC 2019) and the elevation of the CMF to sub-unified command status in 2022 (USCC 2022).

3. And the elevation of Information as the seventh joint function (the Joint Functions are: C2, intelligence, fires, movement and maneuver, protection, sustainment, and information) (JCS 2017, III–1).

This increased emphasis and activity has resulted in updated definitions for the Information Environment and cyberspace:

- DoD defines: "The IE [information environment] is comprised of and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The IE also includes technical systems and their use of data. The IE directly affects and transcends all OE [operational environments]" (JCS 2018b, 42).

- DoD defines cyberspace as: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JCS 2018a, GL-4).

In addition to the updated definitions, the Department has promulgated four cyberspace strategies in the last sixteen years: (JCS 2006), (DoD 2011), (DoD 2015), (DoD 2018), and another is about to be published. Additionally, DoD issued the *Strategy for Operations in the Information Environment* in 2016, (DoD 2016) followed by the Joint Chiefs of Staff declaring information the seventh joint function, as mentioned above, and issuing the *Joint Concept for Operating in the Information Environment* in 2018 (JCS 2018b).

As cyber organizations and definitions matured, scholars and practitioners began questioning the equivalence of nuclear and cyber deterrence, especially those more technically and operationally focused. In 2009, Martin Libicki of RAND warned that "ambiguities of cyber deterrence contrast starkly with the clarities of nuclear deterrence" (Libicki 2009, xiv). Alarming rhetoric continued; in 2011, CIA Director, Leon Panetta, during his testimony for confirmation as Secretary of Defense, repeated warnings that had been circulating for twenty years: "the next Pearl Harbor that we confront could very well be a cyberattack" (Anna Mulrine 2011).

Only in 2018, another decade later, were U.S. offensive cyber operations unleashed from requiring presidential release authority on par with the launch of nuclear weapons (Volz 2018). Shortly afterward, General Paul Nakasone, Commander of USCYBERCOM and Director of the National Security Agency (NSA), confirmed these changes and highlighted four realities in cyberspace: 1) we

are in constant contact with adversaries, 2) our security is challenged, 3) superiority is ephemeral, and 4) advantage favors initiative (Eliason 2019, 4).

These policy changes recognize cyberspace as a domain of constant action to defend actively, conduct reconnaissance, understand capabilities and intent, and improve quickly. Nakasone told lawmakers, "In the last ten years, our adversaries have been operating below the threshold of armed conflict, stealing our intellectual property, leveraging our personally identifiable information, or attempting to influence our elections." USCYBERCOM "evolved its strategic concept and operational approach from a response force to a persistence force" (Eliason 2019, 5).

Instead of reinforcing 'cyber is nuclear,' Nakasone offered new analogies: "We must *defend forward* in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace" (Nakasone 2019, 12). We cannot succeed if our cyber forces and capabilities remain inside of our own networks; we must continuously engage. "Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment" (Nakasone 2019, 12).

Contrary to equating cyber with weapons of mass destruction, then-Defense Secretary Esper asserted, "We are at war in the cyber domain now battling countries like Russia and China who are doing everything from stealing technology to influencing elections to putting out disinformation about the United States" (RM Staff 2019). That contrasts sharply with nuclear weapons and nuclear deterrence; states do not use nuclear weapons–at all–let alone continuously.

Understanding of these recent changes continues to percolate through the military, international relations, and national security policy communities, while policy misunderstandings continue in areas such as cyber deterrence, cyber weapons, cyber targets, and cyber terrain (Smeets 2018). A recent book, *Cyber Persistence Theory* (Fischerkeller, Goldman, and Harknett 2022), builds upon the recent changes expressed by General Nakasone in 2018 and presents an updated theory on competition in cyberspace to guide policymakers. In this context and with the recent release of the new U.S. National Cybersecurity Strategy, prominent voices in the national cyber community shared their thoughts.

Senior Official Thoughts on What We Need to Know

On April 6, 2023, the Atlantic Council's Cyber Statecraft Initiative hosted a panel discussion on the new National Cybersecurity Strategy (NCS). The panel featured

four senior officials: Kemba Walden, Acting National Cyber Director, ONCD at the White House; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA) at DHS; Ambassador Nathaniel Fick, Ambassador at Large for Cyberspace and Digital Policy at DoS; and Marshall Miller, Principal Associate Deputy Attorney General at DoJ (Walden et al. 2023).

The author attended and asked each official to identify the most important elements that policymakers and strategists must understand about cyber. Their responses are paraphrased by the author below to capture meaning and tone.

Kemba Walden, Acting National Cyber ONCD at the White House

> I'll give you three:
>
> 1. First, cyberspace is not just a technology and not just the technology of the CIA triad.[4] It's technology, people, and doctrine.
>
> 2. Second, we must understand risk-in general and risk in cybersecurity. A vulnerability exposes us to threats. A threat is a malicious or negative event that takes advantage of a vulnerability (capability and intent). The risk is the potential for consequences (loss and damage) when the threat occurs. You don't get to zero risk. Cybersecurity is fundamentally an exercise in mitigating risk.
>
> 3. The third piece is focused on how we've constructed the strategy.
>
> Cybersecurity is subordinate to everything else. Cyber enables everything that we want our digital ecosystem to be able to do. It is an all-of-humanity issue. It is not just a national security concern. It's about tech innovations and economic development; at its core cyber helps communities thrive.

Jen Easterly, Director of CISA

> Most important are the two fundamental and game-changing precepts that are articulated in this new National Cybersecurity Strategy.
>
> 1. First, the burden of security must be placed on those most able to bear it.

[4] The CIA (Confidentiality, Integrity, Availability) triad is a fundamental, widely adopted cybersecurity model.

2. Second, we must make long term investments in the safety and security and resilience of our ecosystem.

These very simple but powerful tenets are where the five strategy pillars are derived from and what anybody thinking about cyber policy and cyber strategy would want to use as a grounding foundation.

Amb. Nate Fick, Ambassador at Large for Cyberspace and Digital Policy, DoS

I'll give you the five pieces from the seat of the diplomat.[5]

1. Articulate our positive, compelling, attractive vision because this can't just be anti-China or anti-Russia. We need a more persuasive posture for middle-ground states to join us.

2. Build that coalition, bilaterally and multilaterally. We want in the long term, the greatest number of people, the greatest cumulative GDP, the greatest number of innovative companies, the most collective R&D dollars, we need that on our collective side.

3. For the United States to engage hard in the multilateral fora where the norms and standards are set. I'm sympathetic to the argument that the U.N. is slow and inefficient. The problem is if the U.S. disengages, all it means is others fill the void.

4. Be deliberate about sustaining and defending the areas of advantage that we currently have. This is widening the aperture on cybersecurity. It's also about ICT. It's about the enabling technologies of 6G. It's about quantum science, it's about artificial intelligence.

5. Build the capacity to sustain what I think is going to be a generational strategy. It's not about the people on the stage here, the people in the room here, and it's not about our successors. It's about our successors' successors' successors. This is going to be a long-term game.

Marshall Miller, Principal Associate Deputy Attorney General, DoJ

Look at the tools and authorities we have. Can they meet the moment, or must they be modernized? And if they must be

[5] GDP is Gross Domestic Product, R&D is Research & Development, UN is the United Nations, ICT is Information and Communications Technology, 6G is 6th Generation cellular technology.

> modernized, can it simply be the way we approach the authorities or is legislation required?
>
> A good example is the CFIUS[6] process. CFIUS was created to evaluate the idea of a foreign country buying a brick-and-mortar business. Do we want them to buy that brick-and-mortar business? Do we not? Is it near a military base? How can we use that authority to get at real threats now, for example data security?
>
> Does the tool still work? Can we make it work? And if we can't, how can we modernize it? We must think about that across all kinds of authorities that defend our national security.

Ongoing Research on National Security Cyber Policy

The author was fortunate to hear detailed insights from these four key cyber officials and is thankful for their insights, particularly on the applicability of the new national strategy to their responsibilities. The author's current research is focused on increasing baseline understanding of cyberspace among strategists and policymakers responsible for national security cyber policy. This baseline gap is a known requirement, well-documented by reports from The Government Accountability Office (GAO) report, *Cybersecurity: Clarity of Leadership Urgently Needed* (GAO 2020), the Congressional Research Service (Theohary 2021), and in November 2022 by a RAND report specifically focused on DoD cyber education (Hodgson et al. 2022).

In addition to RAND, think-tanks ranging from the Atlantic Council and CSIS (November 2022 Future of U.S. Cyber and Infrastructure Security) (Easterly et al. 2022) to the Harvard Kennedy School's Belfer Center (2022 Cyber Power Index (Voo, Hemani, and Cassidy 2022)), and the Council on Foreign Relations (October 2022 discussion with CISA Director and CYBERCOM Commander) (Easterly and Nakasone 2022) have frequently sought to illuminate these topics for our community. Furthermore, two of the six pillars of the Congressionally-chartered Cyberspace Solarium Commission contain cyber education recommendations ("Cyberspace Solarium Commission - Report" 2020).

In addition to the new NCS, the *National Security Strategy* (NSS) and the *National Defense Strategy* (NDS), both published in October 2022, re-emphasize cyber. The NSS includes "cyber" 32 times in the 47-page report and specifically

[6] CFIUS is The Committee on Foreign Investment in the United States, an interagency committee authorized to review certain transactions involving foreign investment in the United States that may impact national security.

highlights "Securing Cyberspace" as a "Global Priority" (Biden 2022, 34), while the NDS emphasizes cyber in nearly every major section (Austin 2022).

The cyber policy problems are real, historical, and continuing. Many scholars, practitioners, and oversight organizations report a pervasive wealth of ignorance regarding cyber and related strategically-disruptive emerging technologies. Maturation of such technologies as artificial intelligence, 6G, and quantum may alter the policy environment. To improve national security cyber policy, the author looks forward to sharing the results of continuing research among cyber scholars, organizations, and practitioners.

About the Author

Joseph Hughes Schafer, PhD

Professor, National Defense University, College of Information and Cyberspace

Dr. Joseph H. Schafer is a Professor at NDU's College of Information and Cyberspace where he served as Department Chair and Associate Dean. After his Army career, he served as an executive at Dell and Vice President of L3. He has acquired and operated telecommunications, information, and cybersecurity systems in Iraq, the White House, and the Pentagon. He has a B.S. in Electrical Engineering & Computer Science from West Point; M.S. and Ph.D. in Computer Science from GWU; M.A. in Strategy from Naval War College; and M.B.A. from UVA Darden. He holds CISSP, CEH and QTE certifications and serves on several boards. He has taught in GWU's Cybersecurity M.S. since 2014. At NDU Joseph teaches U.S. and allied Cyber Workforce and War College students. He developed and teaches the Artificial Intelligence and National Security course. Dr. Schafer is currently creating the Framework for National Security Cyber Policy.

Acknowledgment

I thank the Atlantic Council, and particularly Kemba Walden, Jen Easterly, Nate Fick, and Marshall Miller for helping to advance our understanding of cyber policy.

References

Anna Mulrine. 2011. "CIA Chief Leon Panetta: The next Pearl Harbor Could Be a Cyberattack." *Christian Science Monitor*, June 9, 2011. https://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

Austin, Lloyd J., III. 2022. "2022 National Defense Strategy of The United States of America." The Pentagon. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

Biden, Joseph Robinette, Jr. 2022. "National Security Strategy." Washington, DC: The White House. https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.

———. 2023. "National Cybersecurity Strategy." Washington, DC: The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

Bulao, Jacquelyn. 2022. "How Many Cyber Attacks Happen Per Day in 2022?" Techjury. November 26, 2022. https://techjury.net/blog/how-many-cyber-attacks-per-day/.

CSIS. 2022. "Significant Cyber Incidents Since 2006." Washington, DC: Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/221109_Significant_Cyber_Incidents.pdf.

"Cyberspace Solarium Commission - Report." 2020. Washington, DC: Cyberspace Solarium Commission. https://www.solarium.gov/report.

DoD. 2004. "National Military Strategy 2004." The Pentagon: Department of Defense. https://history.defense.gov/Portals/70/Documents/nms/nms2004.pdf.

———. 2011. "Department of Defense Strategy for Operating in Cyberspace [2011]." The Pentagon: Department of Defense. https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy; https://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

———. 2015. "Department of Defense Cyber Strategy [2015]." The Pentagon: Department of Defense. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

———. 2016. "Department of Defense Strategy for Operations in the Information Environment." The Pentagon: Secretary of Defense. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

———. 2018. "Summary | 2018 Department of Defense Cyber Strategy." The Pentagon: Department of Defense. https://www.hsdl.org/?abstract&did=816094.

———. 2022. "DoD Cybersecurity Policy Chart – DoD IACs." December 22, 2022. https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/.

———. 2023. "DoD Cyber Exchange." January 26, 2023. https://public.cyber.mil/.

Easterly, Jen, Ron Green, Valerie Cofield, and Grant Schneider. 2022. CISA Strategic Plan for 2023-2025: The Future of U.S. Cyber and Infrastructure Security | Center for Strategic and International Studies (CSIS) Interview by Suzanne Spaulding and James Andrew Lewis.

https://www.csis.org/events/cisa-strategic-plan-2023-2025-future-us-cyber-and-infrastructure-security.

Easterly, Jen, and Paul M. Nakasone. 2022. Cyber Collaboration in the Age of Hybrid Warfare: A Conversation with Jen Easterly and Paul Nakasone at The Council on Foreign Relations Interview by Dina Temple-Raston. CFR. https://www.cfr.org/event/cyber-collaboration-age-hybrid-warfare-conversation-jen-easterly-and-paul-nakasone.

Eliason, William T. 2019. "An Interview with Paul M. Nakasone (Commander USCYBERCOM)." *Joint Forces Quarterly*, no. 92 (January): 4–9.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. New York: Oxford University Press. https://academic.oup.com/book/41918.

GAO. 2020. "Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy." GAO-20-629. Washington, DC: Government Accountability Office. https://www.gao.gov/products/gao-20-629.

Hodgson, Quentin E., Charles A. Goldman, Jim Mignano, and Karishma R. Mehta. 2022. "Educating for Evolving Operational Domains: Cyber and Information Education in the Department of Defense and the Role of the College of Information and Cyberspace." RAND Corporation. https://doi.org/10.7249/RRA1548-1.

JCS. 2006. "National Military Strategy for Cyberspace Operations [2006 Declassified]." The Pentagon: Joint Chiefs of Staff. https://nsarchive.gwu.edu/sites/default/files/documents/2700103/Document-23.pdf.

———. 2017. "Joint Publication 3-0, Joint Operations." The Pentagon: Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

———. 2018a. "Joint Publication 3-12: Cyberspace Operations." The Pentagon: Joint Chiefs of Staff. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

———. 2018b. "Joint Concept for Operating in the Information Environment (JCOIE)." The Pentagon: Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

Jensen, Eric Talbot. 2017. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law* 48: 44.

Kaplan, Fred. 2017. *Dark Territory: The Secret History of Cyber War*. Reprint edition. New York: Simon & Schuster.

Korzak, Elaine. 2021. "Russia's Cyber Policy Efforts in the United Nations." Tallinn Paper No. 11. Tallinn Paper. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Lavrov, Sergei. 1998. "Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General." New York: United Nations.

Leitzel, Benjamin C and Hillebrand, Gregory D. 2022. "Strategic Cyberspace Operations Guide." Carlisle Barracks, PA: U.S. Army War College, Center for Strategic Leadership. https://csl.armywarcollege.edu/.

Libicki, Martin C. 2009. "Cyberdeterrence and Cyberwar." RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html.

Mitnick, Kevin, Simon, William L., and Wozniak, Steve. 2012. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Back Bay Books. https://www.amazon.com/gp/product/0316037729/.

Nakasone, Paul M., GEN. 2019. "A Cyber Force for Persistent Operations." *Joint Forces Quarterly*, no. 92 (January): 10–14.

RM Staff. 2019. "Esper on Russia: Pentagon Nominee Sees Moscow as 'Strategic Competitor,' 'Potential Adversary.'" *Russia Matters. Harvard Kennedy School's Belfer Center for Science and International Affairs*, July 17, 2019. https://www.russiamatters.org/analysis/esper-russia-pentagon-nominee-sees-moscow-strategic-competitor-potential-adversary.

Schafer, Joseph Hughes. 2020. "The Influence of Information Power Upon the Great Game in Cyberspace." Presented at the 15th International Conference on Cyber Warfare and Security, Old Dominion University, Norfolk, Virginia, USA, February 12. https://www.academic-conferences.org/conferences/iccws.

———. 2023. "Sabbatical Proposal: A Framework for National Security Cyber Policy." Unpublished Research Proposal. Fort McNair, DC: National Defense University.

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Reprint edition. NATO Cooperative Cyber Defence Centre of Excellence. Cambridge; New York: Cambridge University Press.

———, ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd Edition. Cambridge; New York: Cambridge University Press. https://ccdcoe.org/research/tallinn-manual/.

Smeets, Max. 2018. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41 (1–2): 6–32. https://doi.org/10.1080/01402390.2017.1288107.

Soesanto, Stefan, and Max Smeets. 2021. "Cyber Deterrence: The Past, Present, and Future." In *NL ARMS Netherlands Annual Review of Military Studies 2020*, edited by Frans Osinga and Tim Sweijs, 385–400. NL ARMS. The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_20.

Theohary, Catherine A. 2021. "Defense Primer: Cyberspace Operations." CRS Report IF10537. Washington, DC: Congressional Research Service. The

Library of Congress. https://crsreports.congress.gov/product/pdf/IF/IF10537.

USCC. 2019. "U.S. Cyber Command History." U.S. Cyber Command History. 2019. https://www.cybercom.mil/About/History/.

———. 2022. "The Evolution of Cyber: Newest Subordinate Unified Command Is Nation's Joint Cyber Force." U.S. Cyber Command. December 19, 2022. https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe.

Volz, Dustin. 2018. "White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons." *Wall Street Journal*, September 20, 2018, sec. Politics. https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729.

Voo, Julia, Irfan Hemani, and Daniel Cassidy. 2022. "National Cyber Power Index 2022." Cyber Power. Harvard Kennedy School: Belfer Center for Science and International Affairs. www.belfercenter.org/project/cyber-project; https://www.belfercenter.org/publication/national-cyber-power-index-2022.

Walden, Kemba, Jen Easterly, Nathaniel C. Fick, and Marshall Miller. 2023. Rebalancing responsibility: Implementing the National Cybersecurity Strategy Interview by Trey Herr. Panel Discussion. https://www.atlanticcouncil.org/event/rebalancing-responsibility-implementing-the-national-cybersecurity-strategy/.