U.S. Cyber Strategy

An Offensive Realist Perspective

Alejandro Ramos

Alejandro Ramos is a second-year master's candidate in the Security Policy Studies program at The George Washington University's Elliott School of International Affairs. He is concentrating on transnational and cybersecurity issues, with a specific focus on organized crime, insurgencies, and terrorism. Alejandro previously worked as a Corporate Law Paralegal and recently completed a semester-long internship with the International Technology and Trade Associates, Inc., where he gathered and analyzed information for space- and cybersecurity-related projects. For his current capstone project, he is examining Russian influence campaigns in the Balkans with the goal of crafting recommendations for potential use by U.S. or European policymakers.

ABSTRACT

The United States needs a national cybersecurity strategy with a punch. Its adversaries overtly (and covertly) use cyberspace to mold the international world order, attempting to influence domestic and foreign affairs thousands of miles away. Some have even publicly stated that information warfare—to include disinformation and propaganda—is part of their cyber strategy. America must respond accordingly. The U.S. government should design an offensive realist cyber strategy that prevents and counters information warfare, reports on the use of offensive tools and techniques that deny adversarial actions, and shames adversaries who use cyber methods against our country. The U.S.'s rivals and the rest of the world must perceive that its cyber response is powerful, but more importantly, that it is willing to use it to enforce redlines. Without such a strategy, the United States will concede its preeminence in the post-Cold War international world order to rising powers whom take more aggressive cyber actions.

INTRODUCTION

"In the intelligence community you never want to be caught, you want be low and slow, you never really want to be attributed," said Shawn Turskey, head of the Department of Defense's capability and tool development project within U.S. Cyber Command. "But," he emphasized, "there's another space over here, where maybe you definitely want to be louder, where attribution is important to you and you actually want the adversary to know."[1] Turskey is correct: sometimes being loud can be beneficial. In cyberspace, tactics and intentions are often hidden from public view. However, if a country seeks to deter cyberattacks or economic cyberespionage, there will come a point where cyber strategies and tactics will have to be more transparent.

If the United States desires to guard its domestic and international interests from future state-sponsored cyberattacks, it must articulate a robust cybersecurity strategy. U.S. cyber strategy needs to be offensive realist. In short, an offensive realist cyber strategy unveils both the destructive and deterrent powers that cyber operations can provide the United States. It would allow the United States to exploit and respond to its adversaries when attacked, or establish a dominant deterrence posture.

This paper will first establish how cyber tools and cyber policy can be used to affect U.S. foreign policy. Second, it will discuss various offensive, defensive, and deterrent cyber methods that the United States can deploy to follow its offensive realist cyber strategy. These methods include a mix of cyber-based technologies and policy options, including proportional response. Finally, this paper will review an offensive realist cyber strategy and include potential policy recommendations.

CYBER IN INTERNATIONAL SECURITY POLITICS

In the twenty-first century, cyber technologies have enabled both state and non-state actors to become more powerful than they previously were under the traditional international world order. Cyberspace has influenced facets of international relations such as temporality, physicality, permeation, fluidity, participation, attribution, and accountability.[2] Traditionally, physical weapons, military posturing, diplomacy, and other state-related tactics have revolved around one or more of these facets of international relations. But with cyber technologies, U.S. policymakers now can alter foreign relations in ways never thought possible. Countries can use cyber conflict to change the international world order.

In describing a U.S. conflict with China over alleged cyber espionage against American companies, Ryan Maness and Brandon Valeriano, authors of Cyber War versus Cyber Realities: Cyber Conflict in the International System, noted that the U.S. interpretation and potential response to the intrusions marked one of the first times that a cyber incident was similar to an act of war. They said, "This [was] a significant step, because it allows the response to a nonphysical malicious incident in cyberspace to be in the physical, kinetic form…Rarely have we seen nonphysical threats become the source of physical counter threats."[3] In other words, China used its cyber tools to elicit a response from another country. This may have been unintentional because acts of espionage like this are typically meant to be hidden. Nonetheless, the United States government did threaten reprisals for the intrusions, with U.S.

officials going so far as to say that "[the intrusions] constituted an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and as such, may warrant law enforcement actions or economic sanctions against China.[4]

Cyber technologies do not affect the cyber realm only. In fact, what makes cyber space unique to policymakers is its ability to be used both as a warfighting domain and as an arena to make diplomatic changes. Cyber technologies are used to secure global communications, to control weapon systems and autonomous vehicles, and even to defend critical national and military infrastructures. The aforementioned cyber features allow policymakers and militaries to implement their national security strategies electronically and from long distances. Dr. John B. Sheldon, a professional lecturer who is founder and owner of the Torridon Group, a space and cyberspace consultancy, mentioned, "Cyber operations take place in cyberspace and generate cyber power, but they do not serve their own ends; they serve the ends of policy."[5] Or as strategist and senior fellow at New America Peter Singer stated, "Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence."[6] In short, the United States has a great opportunity to use cyberspace and cyberwar as a continuation of policy by other means.

But can cyber tools be used in an offensive realist strategy? Before that analysis, we must first briefly highlight the unique features of offensive realism and show how cybersecurity fits that mold.

Dr. John J. Mearsheimer's idea of offensive realism can help form an impactful U.S. cyber strategy. To borrow his key tenets, an offensive realist cyber strategy should always strive to *obtain offensive military capability, mitigate against ambiguous rival intentions,* and *seek survival in the international system.*[7] The other two tenets, that the international system is anarchic and that great powers are rational actors, are also important to incorporate into the cyber strategy because both highlight two important concepts. First, as a great power, the United States should seek to bring order to this anarchic system. Second, the country should assume foreign governments act rationally. For the latter point specifically, U.S. officials should understand that if they use offensive cyber countermeasures against other states, the victims would respond accordingly. So, if policymakers mount an ill-conceived cyberattack, the United States should be prepared for reprisals.

With cyberspace increasingly becoming a new warfighting domain, the United States must focus more on building cyber capacities that satisfy the tenets of offensive realism outlined above, particularly in both building offensive military capabilities and ensuring the nation's survivability through cyber means. This does not necessarily mean that the country should start a cyberwar. Rather, the United States must build cyber capabilities that provide a robust defense and serve as a deterrent through an overt show of the country's strength and capability.

CYBER POWER: STRENGTH IN AND OUT OF CYBERSPACE

Cyber tactics are indeed covert, but this does not mean that the United States should refrain from publicly using or revealing its cyber capabilities. In fact, by demonstrating some of its cyber techniques, the United States can deter its rivals by showing its strength and its threat capabilities. One country has already done this: China. Since the 2015 release of China's Military Strategy White Paper discussing cyber capabilities, there are reports that the country has used elements of the People's Liberation Army to "steal information from over two dozen Defense Department weapon programs, including the Patriot missile system and the U.S. Navy's new littoral combat ship."[8] These intrusions can be construed as simple espionage, yet their implications are far from simple. They are used to produce military advantages over the United States without developing human assets to steal classified information, let alone ever stepping foot into a research facility. In 2013, the Commissioner of the U.S.-China Economic and Security Review Commission highlighted that China has been conducting these activities to "…fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans," among other sensitive information collection.[9] Although these Chinese cyber intrusions appear part of recently developed cyber strategy, the NATO Cooperative Cyber Defense Centre of Excellence has identified China's cyber strategy as being developed as early as 1986.[10] The Chinese know that the U.S. government is aware of their intrusions, but they persist nonetheless.

Another U.S. rival known to be developing offensive cyber capabilities is Russia. For decades, the Russian government has been developing vast cyber capabilities both for offensive and defensive purposes. Although its government and civilian cyber specialists have been known to conduct a variety of illicit cyber activities, one of Russia's key cyber strategies is based on creating and spreading internet-based content as weaponized information to affect policy decisions in other countries. In 2007, Russia used its cyber forces to attack Estonian banks, parliament, ministries, newspapers, and TV stations after a dispute regarding the relocation of a Russian grave marker that erupted between the Estonian government and its ethnic Russian population. This example has been widely cited as the first publicly recorded instance that a country used its cyber capabilities against another with a plan to disrupt the other's critical infrastructure.[11] The Russians even used their cyber forces to influence the 2016 U.S. presidential election, using a coordinated strategy—ordered by top Russian officials—comprised of online propaganda, covert distribution of malicious e-mails, and media influence operations.[12] Despite being accused of cyber intrusions in multiple European countries and the United States, Russia continues to use these tactics today.

In fact, there are reports indicating that Russia is bolstering its cyber capabilities and operations and increasing its cyber specialists. In early 2017, Russian Defense Minister Sergey Shoigu even confirmed the existence of Russian "information troops" that produce "smart, literate, and effective" propaganda. This group of about 1,000 individuals receives funding of around $300 million to conduct cyber operations.[13] A revelation of this kind by such a high-level official was surprising, as Russian government officials rarely acknowledge disinformation campaigns or attempts to influence the domestic affairs of foreign nations.

The above examples of Chinese and Russian cyber operations elicit some questions. Are these cyber operations effective against the United States? And does the U.S. national cyber strategy need similar offensive cyber tactics? First, it is difficult to gauge whether these attacks were "effective" against the United States, by compromising classified military systems and influencing voter attitudes across America. However, at least part of Russia's influence strategy during the U.S. presidential election seems to have been effective at further polarizing the American public and embarrassing political figures and journalists.[14] China's theft of U.S. military research has also proven successful in producing copies of aircraft like the American Joint Strike Fighter.[15] Therefore, it is safe to assume that these Russian and Chinese tactics have garnered at least some success against the United States.

Yet, the United States seems as if it does not use—or at least does not disclose—similar tactics. If it does not, then U.S. policymakers must seriously consider incorporating similar methods to punish foreign governments for attacking U.S. information technology systems. An aggressive U.S. cyber response provides an appropriate means to exact consequences. However, responding to cyberattacks at the national level is difficult for a variety of reasons. The response depends not only on what the country is responding to, but also on what the equal amount of damage that can be inflicted in self-defense or to deter your rival is. In other words, how can the United States proportionally respond to a cyberattack? With an offensive realist cyber strategy, the proportional response should be aggressive and overt.

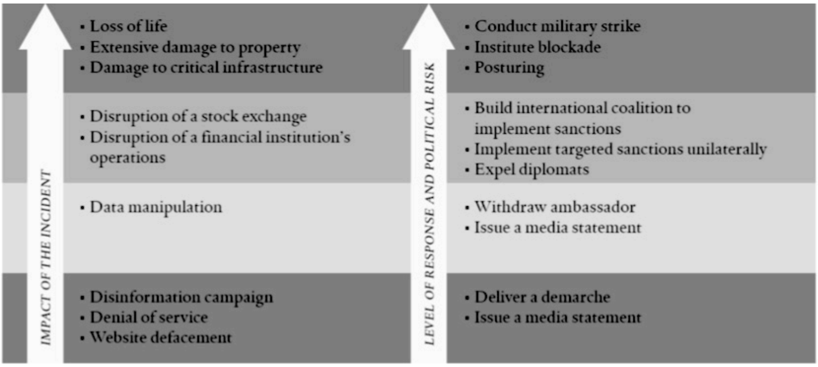
FLEXIBLE "PROPORTIONAL" RESPONSE

Proportional response is a contentious topic in cybersecurity. When formulating military strategy, proportionality is equated with a sort of tit-for-tat. However, in cyberspace, a tit-for-tat response is difficult to create and implement. Factors that make a cyber proportional response hard to determine are attributions of cyberattacks to specific individuals or countries, determining individuals and systems that will inevitably be affected, and gauging how the sanctioned individual or state will respond subsequently. Even if law enforcement authorities identify cyber criminals as the perpetrators of the attacks, the alleged can still deny any involvement, especially if they live in another country or are foreign political leaders. So, what can the United States rely on to provide proper attribution and what would an offensive realist strategy with a flexible proportional response look like?

First, the United States can only trust its own systems and investigators to accurately attribute and create a proportional response. Dr. Tobias Feakin, senior analyst and director at the Australian Strategic Policy Institute, highlighted that "policymakers can only rely on the intelligence community's confidence in its attribution of responsibility, the impact of the incident, and the levers of national power at a state's disposal."[16] In other words, even if attribution is time-consuming, it still can be conducted accurately. Therefore U.S. officials have the flexibility to order a proportional response or a response that exceeds pre-established thresholds. Under an offensive realist cyber strategy, the United States must not hesitate in crafting publicly-acknowledged responses that move beyond proportional thresholds.

But what metrics can policymakers use to construct viable and effective cyber responses? Feakin's illustration of proportional cyber responses (Figure 1) is a good start for policy makers. In the chart below, Feakin outlined a four-pronged escalation ladder demonstrating predetermined responses policymakers could issue. Clearly, losses of life and damage to property and critical infrastructure would garner the strongest response U.S. policymakers could muster. However, the yellow and green zones represent areas where policymakers have more flexibility to create unique responses. Within these two zones, which include data manipulation and disinformation campaigns, there is potential for U.S. policymakers to create tougher responses. For example, under the level of a disinformation campaign, Feakin notes that a demarche or media statement should be issued.

FIGURE 1



• Loss of life • Extensive damage to property • Damage to critical infrastructure	• Conduct military strike • Institute blockade • Posturing
• Disruption of a stock exchange • Disruption of a financial institution's operations	• Build international coalition to implement sanctions • Implement targeted sanctions unilaterally • Expel diplomats
• Data manipulation	• Withdraw ambassador • Issue a media statement
• Disinformation campaign • Denial of service • Website defacement	• Deliver a demarche • Issue a media statement

SOURCE: TOBIAS FEAKIN, "DEVELOPING A PROPORTIONATE RESPONSE TO A CYBER INCIDENT," COUNCIL ON FOREIGN RELATIONS, AUGUST 24, 2015, HTTP://WWW.CFR.ORG/CYBERSECURITY/DEVELOPING-PROPORTIONATE-RESPONSE-CYBER-INCIDENT/P36927.

If the U.S. intends to bolster its cyber offensive capability, it must not rely on demarches and statements that can be easily dismissed by the alleged country and other allies. Considering Russia's influence on the 2016 U.S. election, a U.S offensive realist cyber strategy should entail a tougher response to disinformation campaigns that directly influence domestic policy or U.S. interests throughout the world. When the United States Intelligence Community detects a country like Russia or China conducting active disinformation campaigns against America, U.S. policymakers should release a package of targeted sanctions against the offending country and/or provide military assistance to the rivals of its foes, but only after an accurate attribution has been completed. Furthermore, as indicated in the chart, policymakers should also consider expelling diplomats.

This robust response is meant to punish the offending country, while also deterring further actions. As the world continues to develop more comprehensive technologies, cyber disinformation campaigns, espionage, sabotage, and attacks will increase in number and scale. The United States must act now to prevent these malicious activities from gaining preeminence in international relations.

If the United States is to create a strong offensive realist cyber strategy, what are some of the tools at its disposal? The following describes some of the methods the United States can best deploy to ensure its hegemony and secure its survivability in the international system.

CYBER SURVIVAL

Having a robust offensive realist cyber strategy involves two complementary components: overwhelming offensive capabilities and elaborate defensive countermeasures. A strong offensive capability punishes adversaries for using cyber technologies against the United States, while deterring others from taking actions against the U.S.. Meanwhile, defensive measures allow the United States to prevent and protect critical American technological systems from falling prey to its adversaries. Fortunately, there are offensive and defensive military options already in existence that the United States could incorporate into its cyber strategy.

In defending the U.S. homeland from cyberattacks, the most notable progress made has been through the promotion of public-private partnerships to encourage the exchange of technology updates, information sharing, and threat warnings. Although the National Institute of Standards and Technology established a cybersecurity framework in 2014, it lacks the rigor needed for mandatory implementation because its stipulations on private companies are only voluntary. Today, only about thirty-percent of American companies have adopted the framework since its release, with an expected fifty-percent adoption rate in the next three years.[17]

Luckily, there are other government agencies, such as the Department of Homeland Security and the Department of Defense, that are investing in technologies that provide greater defensive capabilities. For example, DoD's Defense Advanced Research Projects Agency (DARPA) is currently studying decentralized, distributed ledger technology that secures military communications, stores accurate information of data points and equipment, and rapidly detects cyber intrusions. Along with that, the technology makes it more difficult for cyberattacks to gain unauthorized access to U.S military systems.[18] The United States should use cyber technologies and partnerships such as the ones described to safeguard the country.

But what about U.S. interests abroad? How can the United States demonstrate that its offensive cyber tools are credible and can provide its allies with security? The country should develop and deploy more cyber tools capabilities similar to Stuxnet or the alleged U.S. cyber tools currently being used to destroy North Korean missiles, as described below.

If deterrence fails, the United States can use its cyber tools for other purposes. In conflicts, cyber tools can collect and distribute information about rival government spy agencies, diplomatic institutions, military installations, and even top government officials. By doing so, the U.S. can publicly display rivals' malevolent intents which can produce negative consequences on both domestic and international relations for the rival country.

In essence, the United States must articulate a strategy of collecting, manipulating, and disrupting rival electronic processes in cyberspace. Having a formidable offensive realist cyber strategy means having the ability to turn collected information into different effects. Tim Ridout, a fellow at the German Marshall Fund of the United States, refers to these effects as information effects and kinetic effects. Ridout says that information effects are outcomes produced and distributed to electronic systems that enable processes such as situational awareness, communications, and coordinated human action. In contrast, kinetic effects are outcomes that use electronic systems to send commands to robots, weapons, vehicles, and appliances.[19]

To establish a cyber offensive realist approach, the United States should combine information effects and kinetic effects in a policy of cyber offensive action. For information effects, the United States can breach rival systems to manipulate military information such as troop movements, weapon capabilities, and strategy prescriptions. In "spoofing," the United States can use its cyber capabilities to trick rivals into seeing information that is untrue. Furthermore, the United States can also use cyber techniques to generate physical damage to rival systems. The most well-known example of kinetic effects from a cyber weapon is the case of Stuxnet in 2010, when the United States and Israel allegedly developed a computer worm that destroyed Iranian nuclear centrifuges. Although the technology itself is not as noteworthy as the media has portrayed it to be, its physical impact and strategic importance should be highlighted because the program "…opened security researchers' eyes to the fact that malware isn't restricted to computers. Malware can affect critical physical infrastructures, which are mostly controlled by software. This implies that threats might extend to real lives."[20] Stuxnet is a case-in-point of how cyber tools can be used for offensive measures.

The recent spate of North Korean missile launches has also worried multiple U.S. administrations. Yet, since 2013, there have been reports indicating that the United States has a program combining cyber tools, lasers, and other signal jamming techniques that have been able to destroy North Korean missiles before or right after launches.[21] This represents a major turning point since Stuxnet less than a decade earlier. If true, this indicates that the United States has exponentially enhanced its cyber capabilities from targeting one immoveable target to possessing technologies that can be used on multiple targets at multiple locations.

Moreover, it indicates that the United States can also destroy moving targets without firing a single shot, all while remaining undetected. These cyber techniques, if true, can be a perfect match for an offensive realist cyber strategy because it allows the United States to defend its interests abroad (including its allies), exhibits that its offensive, deterrent, and defensive strength remain intact, and solidifies its hegemony in the international system.

Having a policy toolbox filled with both offensive and defensive cyber measures allows the United States to remain in control of its national security, defend its territory, and project influence across the world. Although espionage may seem taboo, rivals to the United States are nonetheless already employing cyber methods of spycraft. This paper advocates for the United States to use the secrets garnered from cyber espionage in a transparent manner to deter its rivals from conducting cyberattacks against the U.S. homeland, its military forces, and allies. This could be thought of as a cyber deterrence strategy, akin to the nuclear deterrence strategies of the Cold War. Although this may increase the potential for cyberattacks on American systems, these already occur daily and are often directed at the most significant agencies, platforms, and institutions in the country, demonstrating the need for urgent action.

CONCLUSION

Russia, China, Iran, and other countries are developing advanced cyber capabilities. Furthermore, individuals worldwide are becoming cognizant of cyber tools, methods, and equipment as governments realize the importance of cyber education. As mentioned, it is evident that individuals and states will continue to grow capabilities that will test U.S. resolve and the international world order. Although U.S. policymakers are currently seeking tougher domestic defensive policies, procedures, and tools, the United States needs a firm offensive national cyber strategy. The following are policy recommendations to establish an effective U.S. offensive realist cyber strategy.

First, on the defensive side of an offensive realist cyber strategy, the U.S. Federal government should continue to work with private companies to share technology trends and threat intelligence, as well as to develop cyber tools to neutralize physical threats. Currently, U.S. President Donald J. Trump has yet to release his national cybersecurity strategy; however there are indications that his would be a continuation of former President Barack Obama's.[22] If this is seen to be true, this may entail an intensification of public-private partnerships. Together, private business and individuals may find it easier to notify law enforcement authorities about cyber threats while the federal government can step in to investigate and neutralize the threats. In fact, if the government cannot step in quick enough, U.S. Representative from Georgia Tom Graves has proposed a bill called the "Active Cyber Defense Certainty Act," enabling citizens and private sector companies to take self-defense measures against threats operating inside their computers.[23]

In addition to defending critical infrastructure and the U.S. homeland, the federal government also needs to invest more resources into developing defensive cyber tools that can protect against missiles or other remote-operated weapons. The supposed cyber tools used to shoot down North Korean missiles, though not confirmed, seem like the correct step in this direction. Developing cyber technologies that can mitigate threats from state and non-state actors is critical to U.S. interests. This gives the United States flexibility in deterring attacks without necessarily risking lives or escalating tensions. Although these cyber tools may be costly, they provide the country greater returns for a lower risk.

Yet, along with defensive cyber weaponry and policies, the United States should also develop offensive cyber weapons. These weapons could manipulate data, computers, and other electronic devices belonging to rivals, both during peacetime and wartime. Additionally, the United States should revamp propaganda campaigns like the media strategies used in Europe during the Cold War, such as Radio Free Liberty and Radio Free Europe, by creating propaganda disseminated throughout the Internet belonging to rival nations. If rivals like Russia can manufacture online propaganda campaigns, then the United States should also be willing to conduct similar campaigns. The American version of these campaigns could tout democracy, report relevant facts, or positively influence foreign populations across the globe.

Lastly, U.S. officials must move quickly to establish a single command to coordinate all aspects of military cyber capabilities and strategy. Currently, U.S. Cyber Command is in limbo. In December 2016, the U.S. Congress passed a bill that elevated Cyber Command to a unified combatant command, splitting it away from U.S. Strategic Command.[24] During August of 2017, under a Presidential executive order, Secretary of Defense James Mattis began the process of elevating Cyber Command into a unified combatant command.[25] However, the director of the National Security Agency, U.S. Navy Admiral Mike Rogers, continues to lead both institutions. This confusion can only be solved after the DoD has fully assessed whether the command has the capacity to be a standalone agency—a process that is still ongoing.[26] Splitting the office away from the NSA and establishing it as a single command, with its own facilities and leader, will allow the United States to coordinate and implement a coherent national cyber strategy throughout all of the U.S. Armed Forces and the nation. Without this coordination, variation in the cyber strategy of the military forces will prove detrimental to a national offensive realist cyber strategy.

This new administration, which is still working to produce a clear national cybersecurity strategy, has the opportunity to adopt a strategy that demonstrates strength, defends U.S. interests, and matches conventional deterrence with cyber tools. Without a more aggressive cyber strategy, Russia, China, and other actors, will continue to undermine U.S. survivability and power in both cyberspace and the international arena.

ENDNOTES

[1] Chris Bing, "U.S. Cyber Command director: We want 'loud,' offensive cyber tools," *FedScoop*, 30 Aug 2016, https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016.

[2] Nazli Choucri, "Emerging Trends in Cyberspace: Dimensions & Dilemmas," White paper presented at the 2012 Conference called "Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition," University of Pittsburgh, https://ecir.mit.edu/sites/default/files/documents/%5BChoucri%5D%202012%20Emerging%20Trends%20in%20Cyberspace-Dimensions%20%26%20Dilemmas.pdf, 2.

[3] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," Armed Forces & Society, Vol. 42, no. 2 (2016), http://journals.sagepub.com.proxygw.wrlc.org/doi/pdf/10.1177/0095327X15572997, 303.

[4] John Rollins, "U.S.–China Cyber Agreement," Congressional Research Service, 16 Oct 2015, https://fas.org/sgp/crs/row/IN10376.pdf, 3.

[5] John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," In Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Ed. by Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), http://www.jstor.org.proxygw.wrlc.org/stable/pdf/j.ctt2tt6rz.17.pdf, 209.

[6] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York: Oxford University Press, 2014), 121.

[7] John J. Mearsheimer, *The Tragedy of Great Power Politics*, Chapter: "Anarchy and the Struggle for Power," (New York: W.W. Norton, 2001), 30-31.

[8] Adam Segal, "How China is preparing for cyberwar," *The Christian Science Monitor*, 20 Mar 2017, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.

9 Testimony prepared by Larry M. Wortzel before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, 9 Jul 2013, http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf, 1.

10 Mikk Raud, “China and Cyber: Attitudes, Strategies, Organisation,” NATO Cooperative Cyber Defense Centre of Excellence, August 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf, 11.

11 Scheherazade Rehman, “Estonia's Lessons in Cyberwarfare,” *U.S. News & World Report*, 14 Jan 2013, https://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare.

12 “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution,” U.S. Office of the Director of National Intelligence, 6 Jan 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

13 Sam Jones, “Russia mobilises an elite band of cyber warriors,” *Financial Times*, 23 Feb 2017, https://www.ft.com/content/f41e1dc4-ef83-11e6-ba01-119a44939bb6.

14 Philip Ewing, “Charges, Hearings Sharpen The Big Picture About Russia’s Influence Campaign,” *NPR*, 1 Nov 2017, https://www.npr.org/2017/11/01/561203044/charges-hearings-sharpen-the-big-picture-about-russias-influence-campaign

15 Eric Lichtblau, “C.I.A. Had Evidence of Russian Effort to Help Trump Earlier Than Believed,” The *New York Times*, 6 Apr 2017, https://www.nytimes.com/2017/04/06/us/trump-russia-cia-john-brennan.html and Marcus Weisgerber, “China’s Copycat Jet Raises Questions About F-35,” Defense One, September 23, 2015, http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859.

16 Tobias Feakin, “Developing a Proportionate Response to a Cyber Incident,” Council on Foreign Relations, August 24, 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

17 Joseph Marks, “Industry Urges Changes to NIST Framework Update,” *Nextgov*, 11 Apr 2017, http://www.nextgov.com/cybersecurity/2017/04/industry-urges-changes-nist-framework-update/136933.

18 Stan Higgins, “DARPA Seeks Blockchain Messaging System for Battlefield Use,” CoinDesk, 25 Apr 2016, http://www.coindesk.com/darpa-seeks-blockchain-messaging-system-for-battlefield-back-office-use.

19 Tim Ridout, “Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience,” The Fletcher Forum of World Affairs, Vol. 40, No. 2 (2016), 66.

20 Thomas M. Chen and Saeed Abu-Nimeh, “Lessons from Stuxnet,” IEEE Computer Society, April 2011, http://ieeexplore.ieee.org.proxygw.wrlc.org/stamp/stamp.jsp?arnumber=5742014, 93.

21 See: David E. Sanger and William J. Broad, “Hand of U.S. Leaves North Korea’s Missile Program Shaken,” The New York Times, April 18, 2017, https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html and David E. Sanger and William J. Broad, “Trump Inherits a Secret Cyberwar Against North Korean Missiles,” *The New York Times*, 4 Mar 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

22 Joseph Marks, “White House Wants to Bake Security into New IT Projects,” *Defense One*, 25 APr 2017, http://www.defenseone.com/politics/2017/04/white-house-wants-bake-security-new-it-projects/137290.

23 Representative Tom Graves (R-Ga.), “Rep. Tom Graves Proposes Cyber Self Defense Bill,” Press Release, March 3, 2017, http://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398726.

24 Morgan Chalfant, “Pentagon mulling split of NSA, Cyber Command,” *The Hill*, 23 Feb 2017, http://thehill.com/policy/cybersecurity/320736-pentagon-mulling-split-of-nsa-cyber-command.

[25] Jim Garamone and Lisa Ferdinando, “DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command,” Defense Media Activity, 18 Aug 2017, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command.

[26] Ibid.