1-1-2018

Cyber

Center on Irregular Warfare & Armed Groups

Center on Irregular Warfare and Armed Groups Reading List 2018

Cyberwarfare & Cybersecurity

Table of Contents

LAST UPDATED: April 2018

Introduction/Background Information

CYBERWARFARE & CYBERSECURITY OVERVIEW

Kang, Lin Yang. "The Threat, Defense, and Control of Cyber Warfare." *Center for International Maritime Security*, April 17, 2017. http://cimsec.org/threat-defense-control-cyber-warfare/32106

This paper looks to present the dangers of cyberattacks and provide an outline of cyberdefense. The author begins by comparing cyberwarfare to special operations. They are both stealthy, difficult to detect attacks that are launched by covert forces. Small-scale cyberattacks can result in large-scale real-world damage. The high-yield, low-risk nature of cyberattacks appeals to non-state actors and state actors alike. The lack of concrete international laws regarding cyberwarfare often allows perpetrators to act with impunity.

Malekos Smith, Jessica. "Twilight Zone Conflicts: Employing Gray Tactics in Cyber Operations." Small Wars Journal. October 27, 2016. http://smallwarsjournal.com/jrnl/art/twilight-zone-conflicts-employing-gray-tactics-in-cyber-operations.

This article explores how Gray Zone Tactics and Hybrid Warfare are implemented through cyber operations. Revisionist powers that wish to change the international order can employ cyber operations as a tool to further their ambitions, as an unregulated cyberspace is easily influenced with minimal cost associated with a failed attack. Cyber operations can be an impactful political instrument that can be launched by third parties, or against various targets that may not be directly associated with the intended adversary.

Štitilis, Darius, Paulius Pakutinskas, Uldis Kinis, and Inga Malinauskaitė. 2016. "Concepts and Principles of Cyber Security Strategies." *Journal of Security & Sustainability* 6, no. 2 (2016):197-210. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=120915722&site=ehost-live

Cyber threats have evolved and expanded and in turn the areas impacted or at risk have expanded as well. The realm of cyberattacks has expanded from individuals and business to states, regions, general infrastructure and governments. Cyberattacks and even cyber wars have become more prevalent than their physical counterparts and need to be properly prepared for and countered. This piece seeks to evaluate different Cyber Security Strategies in governments, how effective they are, and do they have the legal ability to hold individuals or other governments accountable.

White, Josh. "Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies."*Global Security Studies* 7, no. 4 (Fall, 2016): 23-

33.http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=119212350&site=ehost-live

This paper seeks to provide awareness of different cyber threats on both an individual and statewide level. Following this, it suggest security measures that should be adopted on both those levels in order to combat current and future cyber threats. The importance of having a solid understanding of the growth and development of cyber threats is discussed along with past occurrences of cyberattacks both locally and internationally, and the security measures adopted afterwards; however, the rapid advancement of technology makes this difficult to keep up with.

Nye, Joseph S. "Cyber Power." Belfer Center for Science and International Affairs, Harvard Kennedy School,. March 2010. https://www.belfercenter.org/publication/cyber-power.

In the new cyber battlespace, power is no longer measured by the size of armies or economic stature. Power is measured in the capacity to wield influence in cyberspace and smaller state actors are able to decrease the power deficit between themselves and larger state actors. Additionally, cyber allows nonstate actors and proxy actors to have more capability to inflict direct damage upon state actors that they otherwise would have been unable to perpetrate prior to the modern digital age. The balance of power is being redefined by the introduction of the new context of cyber power.

CYBERSECURITY TACTICS AND STRATEGIES

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies*26, no. 3 (May 08, 2018): 452-81. https://www.tandfonline.com/doi/pdf/10.1080/09636412.2017.1306396.

The article assesses the effectiveness of cyberspace as a medium to coerce and influence politics between state and non-state actors. Their findings suggest that many tactics employed by state while effective hybrid strategies do not often coerce the desired political action from the target. Instead, it takes a certain level of cyber intrusion to incur a response. To reach the desired effect, an attack must employ, “attrition, denial, or decapitation strategies.” Much of these tactics target critical infrastructure that civilians rely on, and may lead to further international regulation and institutional normative behavior.

"Cyber Security Strategy Documents." NATO Cooperative Cyber Defence Centre of Excellence. January 22, 2018. https://ccdcoe.org/cyber-security-strategy-documents.html.

This list created by the NATO Cooperative Cyber Defence Centre of Excellence is a compilation of all known national cyber security policy and legal documents that address the cyber domain. The list is updated periodically and focuses on NATO

partners, but other major cyber actors with published doctrines and strategies are included in the product.

Libicki, Martin A. "Strategic Implications of Operational Cyberwar." In *Cyberspace in Peace and War*, 168-78. Annapolis, MD: Naval Institute Press, 2016.

This excerpt (chapter 15) requires USNWC library access or a copy of the book. This chapter from Cyberspace in Peace and War, explores three strategic implications of an operational cyberwar. First, the influence of cyberwar on the digitization strategies of other states. Second, military strategies that "operational cyberwar can shift the correlation of forces." Third, the challenges of a decentralized defense in a cyberwar when attempting to coordinate with and protect allies. NATO and the U.S. are the two central figures in allied cyber defense; however, private corporations now play a role in the defense of key critical infrastructure and networked systems that allied nations rely on.

Large Scale Cyberattacks & State Cyber Capabilities

UKRAINIAN POWER GRID (2015)

Buchanan, Ben . "Cyber Attacks on Ukraine's Power Grid: To What End?" International Institute for Strategic Studies. February 03, 2017. https://www.iiss.org/en/politics%20and%20strategy/blogsections/2017-6dda/february-88e4/cyber-attacks-on-ukraines-power-grid-00d9.

In 2015 a cyberattack targeting one of Ukraine's major power grid left nearly 250,000 people without power. The attack is a prominent reminder of the capability of cyber warfare when targeting a state's critical infrastructure and underscores the need for defending and hardening such vulnerable infrastructure. Investigators determined that the hackers could have caused more damage but it was likely a demonstration of power or capability for the responsible party. The significance for western states, is that the Ukraine "uses equipment and security protections of the same vendors as everybody else around the world," highlighting the potential for a significant vulnerability worldwide to critical infrastructure.

DUQU 2.0 (2015)

Paganini, Pierluigi. "Duqu 2.0: The Most Sophisticated Malware Ever Seen." *INFOSEC Institute*. June 17, 2015. http://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/#gref

The second "strain" of the Duqu malware proved to be more sophisticated and came from a similar source as the original based on similarities in structure to the first Duqu. There is no definitive proof of the malware's origins besides its similarities to other malware but the passkeys and other aspects utilized mimicked those of independent

hacking organizations in order to obstruct the origins of the malware. This attack was of note, not only due to its targeting of countries involved in the negotiations of the P5+1 Iranian nuclear deal and several Middle Eastern countries but that it directly targeted, the security IT company, Kaspersky Labs.

DUQU (2011)

"Iran Says it has 'Controlled' Duqu Malware Attack." *BBC*, November 14, 2011. http://www.bbc.com/news/technology-15721839

The cyberattack, dubbed "Duqu" acted as a scouting mission on targeted computers. It is believed that eight countries were impacted by this spyware, with Iran's nuclear facilities being the primary target. Duqu infiltrated the targeted system via an email depicted to appear as an official document. Once the code had embedded itself in a particular computer it could be used to gather information, infect other networked computers, and leave modules behind that allow additional instructions to be sent to the program to tell it do collect different data or do different things, or to allow for the easier introduction of a new virus using the installed module.

FLAME (2012)

Lee, David. "Flame: Massive Cyber-Attack Discovered Researchers Say." *BBC*, May 28, 2012. http://www.bbc.com/news/technology-18238326

A piece of malware, known as "Flame" due to the command word being used frequently in the code, was discovered in 2012 by Kaspersky Labs. The malware which they believe had been active since 2010, targeted computers in Iran, Sudan, Syria, Lebanon, Saudi Arabia, Egypt, and parts of Israel with the goal of stealing information and monitoring conversations. This was an active piece of software, once it infected a machine, the operators could issue commands to the machine and give it new instructions. Kaspersky believed that this was a state-sponsored malware due to its complexity, selection of its targets, and type of information it was looking for.

STUXNET

Kelley, Michael B. "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*, November 20, 2013. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

The Stuxnet worm was a highly effective and innovative cyber weapon. The article describes a worm that caused the destruction of one-fifth of Iran's uranium enrichment centrifuges at the Natanz plant, and created an entire electronic blueprint of the entire nuclear plant. Stuxnet was introduced through an usb drive into one of the Natanz plant's computers where it then used the blueprint it created to understand how the

plant's control and diagnostic systems worked. Using this information it slowly sped up the reactors until they reached critical levels and broke down, all the while sending normal operating information to the control panels. This was believed to be a joint U.S. and Israeli operation that was introduced in phases. One of the worm's creators commented on the ease of introducing the worm via a thumbdrive, "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

Espionage

Commercial Sabotage and Economic Espionage

Martemucci, Matteo G, USAF. "Unpunished Insults-The Looming Cyber Barbary Wars." *Case Western Reserve Journal of International Law* 47 (Spring, 2015):53-62. https://search.proquest.com/docview/1696876925?accountid=322

Col. Martemucci evaluates the role the U.S. military and government played in protecting American commerce from the Barbary pirates in the early 19th century to the current cyberspace threats against American commerce, especially from China. He argues that there is a role for the DoD and the U.S. Government in the protection of online commerce, but it would only be feasible with high levels of cooperation, information sharing, and a well regulated, transparent, agreement between the government, commercial industries, and the public.

Information Operations

Soshnikov, Andrei. "Inside a Pro-Russia Propaganda Machine in Ukraine." *BBC*, November 13, 2017. http://www.bbc.com/news/blogs-trending-41915295

A Russian propaganda unit, commonly known as the "troll factory" has been working in conjunction with a group out of the self-proclaimed Donetsk People's Republic that calls itself the Russian Liberation Movement. These groups have been creating fake news stories and propaganda videos pretending to be members of extremist groups from Ukraine. They claim to be responsible for attacks in Russia or members of fascist organizations operating out of Kiev, or even part of ISIS employed to fight by the Ukrainian government.

Chen, Adrian. "The Agency." *New York Times Magazine*, June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html

Russian propaganda factories are state sponsored offices where workers are paid for promoting Russian propaganda and values and denouncing Western ideologies. They are the foundation of Russian information operations and are key to controlling the narrative and influencing social dialogue on key salient issues. This article explores how these organizations conduct information campaigns on behalf of the Russian state.

Walker, Shaun. “Salutin’ Putin: inside a Russian troll house.” *Guardian*, April 2, 2015. https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

Former workers talk about how bloggers are paid to use forums and social networks at home and abroad to promote anti-Western and pro-Kremlin commentary and ideologies. These bloggers push state-sponsored content under the guise of regular civilians to sway popular opinion in Russia.

CYBER TERRORISM

Ward, Antonia. "Bitcoin and the Dark Web: The New Terrorist Threat?" Rand. January 22, 2018. https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html.

Bitcoin is most recognizably viewed as a powerful investment and asset, but due to its lack of central repository or administrator, it is often used for fraud and organized crime. The EU has introduced regulations and will begin to monitor and crackdown on cryptocurrencies under the premise of counterterrorism operations as arms dealers on the dark web are using the cryptocurrencies as their primary form of transaction. Jihadist groups are using cryptocurrencies due to its convenience as a replacement for ‘hawala’ so that brokers no longer need to transfer money physically from place to place.

Kenny, Michael. “Cyber-Terrorism in a Post-Stuxnet World.” *Orbis* 59, no. 1 (Winter, 2015):111-128. http://doi.org/10.1016/j.orbis.2014.11.009

This article focuses on how cyberterrorism is its own unique threat and should not be haphazardly placed in the same category as cybercrime, cyberattacks, cyberwarfare, or hacking/hacktivist activities. Cyberterrorism is in essence the use of digital means to conduct a terrorist attack. Shutting down power grids, turning off vital transportation direction systems or impacting water supplies are examples of what cyberterrorism would be akin to. The article to gives definitions and descriptions of cyberattacks, cyberwarfare, hacktivism and cyberterrorism and show that while they all belong in the same “genus” of online attacks, and share some similar characteristics, cyberterrorism along is designed to cause widespread fear or physical intimidation and produce physical violence and individuals and infrastructure. A chart is provided comparing the different attributes of each type of cyberattack.

ISLAMIC STATE

Clarke, Colin P., and Chad C. Serena. "What Happens After ISIS Goes Underground." National Interest. May 29, 2017. http://nationalinterest.org/feature/what-happens-after-isis-goes-underground-20881?page=show.

ISIS continues to lose territory in kinetic battles against coalition partners and anti-extremist operations across the globe. The group has been forced to reevaluate its ability to sustain itself against conventional forces and has once again through its propaganda and social media channels called on a global movement to conduct widespread attacks in western nations. ISIS is in a struggle to survive is transitioning back to an underground insurgency with global affiliates. Part of this plan could be to use the accessible cyberspace to launch new forms of attacks against COIN forces. Part of this effort to improve their cyber capabilities could be to leverage cyber crypto currencies as their new means of primary financial funding. ISIS has proven that they are able to evolve to meet the challenges of modern warfare, using drones to drop explosives, conduct advanced propaganda campaigns, and govern territories and collect taxes. The next phase of their evolution points towards an emphasis on cyber operations.

Clarke, Colin P., and Isaac R. Porche III. "The Online Fight Against ISIS." Rand. April 1, 2016. https://www.rand.org/blog/2016/04/the-online-fight-against-isis.html.

As ISIS loses its foothold in the Middle East, ISIS is seeking to enter the cyber battlespace and attack vulnerable infrastructure in coalition states. Non-state actors have few limitations preventing them from being able to effectively conduct attacks from the cyber domain. As we continue to advance in the digital age, cyber mercenaries and armed groups will develop new and sophisticated methods of financing their operations and launching attacks. Coalition forces will need to forge a strategy that identifies vulnerable critical infrastructure and develop offensive capabilities to mitigate the potential damage ISIS hackers could inflict on allied forces.

Brown, Michael A., and Daniel M. Gerstein. "Anonymous vs. ISIS: Wishing the Vigilante Hackers Luck Against the Murderous Jihadists." Rand. December 14, 2015. https://www.rand.org/blog/2015/12/anonymous-vs-isis-wishing-the-vigilante-hackers-luck.html.

The Hackers and self-proclaimed vigilantes known as Anonymous are taking their fight to ISIS. The hackers have begun assaulting the jihadist group's social media channels and other public outreach. While non-state actors combating ISIS is not a new phenomenon, it is the first time that non-state groups have clashed over cyberspace. Anonymous' attack on ISIS could be used by coalition forces as an example of how to exploit vulnerabilities that ISIS may have in its cyber presence.

Russia

CAPABILITY, INITIATIVES, AND POLICIES

Tucker, Patrick. "If War Comes, Russia Could Disconnect from the Internet. Yes, the Entire

Country." *Nextgov*, March 12, 2018. http://www.nextgov.com/cybersecurity/2018/03/if-war-comes-russia-could-disconnect-internet-yes-entire-country/146589/.

In an effort to harden Russian defense against cyber threats, Russia has transitioned much of its online infrastructure to internal networks that would prohibit unauthorized access from key servers in the event of a breech. The effort took two years of network overhauls, the reduced dependence on outside information technology and ability to unplug Russian military tech from the outside gives Russia an edge should the state enter conflict with another technologically advanced power.

ESTONIA DDOS ATTACK 2007

Alenius, Kari. "An Exceptional War That Ended in Victory for Estonia or an Ordinary e-Disturbance? Estonian Narratives of the Cyber-Attacks in 2007." *European Conference on Information Warfare and Security*. (July, 2012): 18-24, VIII. http://search.proquest.com/docview/1035293217/fulltextPDF/FF9AC32A623C47B6PQ/1?accountid=322

In 2007, Estonia was on the receiving end of daily cyberattacks for several weeks in response to the moving of a memorial to Russian forces. Street protests erupted by Russian speaking residents when the move was announced and soon after on April 27, the cyberattacks began. The attacks mainly targeted Estonian government institutions with a variety of spamming and direct denial of service (DDOS) attacks. The sophistication and organization of these attacks leads to suspicion of the Russian government (since some of the attacks originated directly from Russian government buildings), which Moscow denies despite having previously warned Estonia not to move the statute.

CYBER ATTACK ON GEORGIA PRE-INVASION 2008

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 2010. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

In order to destabilize the Georgian military, Russia launched a coordinated cyberattack in congress with their military invasion. This was an unprecedented action as it was the first joint cyber and kinetic attack. The targets included communication and finance website which left Georgian citizens unable to receive information or instructions and created large scale confusion and distraction which impacted the Georgian government's response to the aggression.

RUSSIAN AGGRESSION

Marks, Joseph. "Once Stealthy, Russian Hackers Now Go Toe to Toe with US Defenders"

Defense One, March 22, 2017. http://www.defenseone.com/politics/2017/03/once-stealthy-russian-hackers-now-go-toe-toe-us-defenders/136374/?oref=d-river

In late 2015, the typical behavior of Russian hackers changed. Normally when caught or confronted online, they would retreat from the system with whatever they could grab, yet they had started to become more assertive. These hackers would stay and try to counteract or block the NSA agents' response and continue their work. While the NSA would not name the specific actors, private firms would around this same time, FireEye, a cybersecurity company reported similar actions being undertaken by Russian hackers. They were no longer running, but had been emboldened and were pushing back and not bothering to clean up their trails. It seemed that at times, they wanted their capabilities to be known.

Maldre, Patrik. "The Russian Cyber Threat: Views from Estonia." *Europe's Edge*, Center for European Policy Analysis (CEPA). May 18, 2016. http://cepa.org/The-Russian-Cyber-Threat-Views-from-Estonia

The small country of Estonia has become a leader in cyber defense through necessity. Russia has been targeting Estonia and other countries in the area for close to a decade. The agencies responsible for Estonian cyber security issued a report claiming that "in cyberspace, Russia is the source of the greatest threat to Estonia, the European Union and NATO. The FSB is believed to spend up to $250 million a year on professional cyber threat actors with the goal of disrupting foreign command and control systems and damaging infrastructure.

Curran, John. "DoJ Charges Russian Government Security Officials in Yahoo Hack." *Cybersecurity Policy Report*. (March 20, 2017):1. http://search.proquest.com/docview/1880365862/2CD05747B4AB41C6PQ/4?accountid=322

Indictments of four people, including members of the Russian FSB were announced by the DOJ in response to the hacking of Yahoo and the theft of a large number of subscribers' e-mails and information. Attorney General Jeff Sessions reaffirmed a commitment to identifying and prosecuting those responsible for future cyberattacks. In addition, members of Congress called for further investigation into the attack in order to gain valuable information about how Russian cyber operations are conducted and also for private companies to be more forthcoming and cooperative with the Government.

China

CHINESE CYBER SECURITY STRATEGY

Kowalewski, Annie. "China's Evolving Cybersecurity Strategy." Georgetown Security Studies

Review. October 27, 2017. http://georgetownsecuritystudiesreview.org/2017/10/27/chinas-evolving-cybersecurity-strategy/.

This article explores China's doctrine, training, and efforts in the cyber domain. China is placing an increased emphasis is reforming their military to adapt to contemporary military strategies by integrating cyber security as a cornerstone of its new doctrine. Information wars and influence operations are important aspects of modern military conflict and China's organizational restructuring of their cyber, space, and electromagnetic forces is an attempt to consolidate and improve upon these domains by creating a new military branch dedicated to those efforts.

Kania, Elsa, Samm Sacks, Paul Triolo, and Graham Webster. "China's Strategic Thinking on Building Power in Cyberspace." New America. September 25, 2017. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

This article is a comprehensive outline and translation of the key points in China's new cyber strategy. "China's strategy calls for developing capabilities and governance capacity in four major baskets: managing internet content and creating "positive energy" online; ensuring general cybersecurity, including protecting critical information infrastructure; developing an independent, domestic technological base for the hardware and software that undergird of the Internet in China; and increasing China's role in building, governing, and operating the Internet globally." China's latest efforts focus on their ability to influence the internet internationally and become a global power in the cyber domain.

JAPAN'S COUNTER STRATEGY

Lui, Helen. "Japan's Cybersecurity Strategy: Deterring China with Selective Engagements." Henry M. Jackson School of International Studies. May 17, 2017. https://jsis.washington.edu/news/japans-cybersecurity-strategy-deterring-china-selective-engagements/.

Japan has increased its cyber capabilities in response to its concerns with China, Russia, and North Korea. Distrust between Japan and China has prevented a political dialogue over normative behavior in the cyber domain and Japan's development of cyber institutions is reflective of their concern for China's assertive posture in the cyber domain. Japan's efforts to keep stride with China and become a major player in the cyber domain is parallel with their national defense spending and efforts to become more militarized.

CHINESE CYBER CAPABILITIES

Nye, Joseph. "Can China Be Deterred in Cyber Space?" The Diplomat. February 3, 2016.

https://thediplomat.com/2016/02/can-china-be-deterred-in-cyber-space/.

Due to the nature of international institutions, political influence, and state reputation, it is often easier to deter state actors from committing cyberattacks than non-state actors. Economic interdependence between China and the United States has largely deterred China from acting against U.S. infrastructure or economic holdings. States that don't have the same level of interdependence may be more inclined to use cyber techniques to harm other states, but sanctions issued by powerful adversaries such as the U.S. on states like North Korea is an effective tool to increase costs in the decision-making process. Hardening cyber defenses is a necessary strategy to mitigate damage from cyberattacks, but perhaps more effective against state sponsored cyberattacks are the political tools wielded by actors in the international system.

OPM HACK

Koerner, Brendan I. "Inside the Cyberattack that Shocked the U.S. Government." *WIRED*. October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

The Massive data breach from individuals operating out of China compromised the highly sensitive information of a large portion of government employees. This article goes into great detail regarding how the attackers accessed the information, how the breach was found out and the countless hours of work spent on countering the breach.

North Korea

CYBER CAPABILITY

Valeriano, Brandon, and Benjamin Jensen. "North Korea's Offensive Cyber Program Might Be Good, But Is it Effective?" Council on Foreign Relations. October 25, 2017. https://www.cfr.org/blog/north-koreas-offensive-cyber-program-might-be-good-it-effective.

North Korea's offensive cyber program may not be the veiled giant that some suggest. The program has not yet inflicted extensive damage on adversarial state actors, but it has been linked to high profile hacking attacks such as "WannaCry" and "Sony 2013". Their success cannot yet be measured politically, and the article estimates they have only managed to steal $81 million. While their cyber operations are cheap and provide valuable international influence, the author suggests that there is little, "actual demonstrated ability to achieve leverage through cyber operations."

SONY HACK 2013

Sanger, David E. and Martin Fackler. "N.S.A. Breached North Korean Networks before Sony Attack, Officials Say." *New York Times*, January 18, 2015.

https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

A North Korean defector told U.S. government officials that North Korea has been perfecting its hacking and cyberattacking abilities over the past 30 years. They have developed techniques aimed towards breaching the systems of individual countries. The NSA had managed to infiltrate this network and monitor some of the computers utilized on it. Sony Pictures was hacked and its information and emails publicized in response to an upcoming movie that depicted a fictional assassination of Kim Jong Un. This was a unique case in which the U.S. directly blamed another nation for a cyberattack.

Iran

IRANIAN CYBER CAPABILITIES

Herr, Trey, and Laura K. Bate. "The Iranian Cyberthreat is Real." Foreign Policy. July 26, 2017. http://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real/.

Cyber operations and attacks in the Middle East have change the dynamics of politics among neighbors. As states use the proxy conflicts in Yemen and Syria as kinetic expressions of force, a battle over cyberspace is unfolding between regional powers. Iran, having been the target of cyberattacks, are now capable of wielding their own influence in cyberspace. Techniques such as defacements, censorship, information controls, espionage campaigns, multifaceted attacks, social media manipulation, and infrastructure attacks are all tools in the Iranian cyber weapons bag.

Adelkhah, Nima. "Iran and Its Cyber-Terrorism Strategies." Jamestown Foundation. May 16, 2016. https://jamestown.org/program/iran-and-its-cyber-terrorism-strategies/.

Iran's employment of offensive cyber operations against the U.S. and its allies have been conducted either directly or through the use of proxies. The attacks have dated back to 2009 and have spanned from attacks on infrastructure and businesses to complex information operations. Iran's defensive posture stems from suspected efforts by the United States and Israel intended to undermine the political institutions of the Iranian government. Iran describes these efforts as cyber-terrorism, and the article identifies two forms of cyberattacks that Iran defends against. The first are "soft" attacks, which are conducted through information operations intended to influence the values and belief systems of the targeted population. The second, are "hard" attacks, which are directed hacking efforts against infrastructure or websites with the intent of denying service.

Libicki, Martin. "Iran: A Rising Cyber Power?" Cipher Brief. December 15, 2015. https://www.thecipherbrief.com/article/cyber/iran-a-rising-cyber-power.

According to the Article, Iran leverages its influence over the cyber domain to achieve four primary objectives. “First, Iran wants to keep its citizens under surveillance. Second, Iran wants to know the intentions and capabilities of other countries. Third, Iran wants a capability to harass those it sees as its foes. Fourth, it may be preparing larger attacks.”

2012 Attack on Saudi Arabia’s National Oil and Gas Utility – Shamoon Attack

Bronk, Christopher. and Eneken Tikk-Ringas. “The Cyber Attack on Saudi Aramco.” *Survival* 55, no. 2 (April 3, 2013): 81-96. http://dx.doi.org/10.1080/00396338.2013.784468

Saudi Arabia’s national oil and gas producer, Aramco, suffered a cyberattack on August 15, 2012 which infected up to 30,000 of its computers with a self-replicating virus. The virus, later referred to as Shamoon, resulted in wholesale deletion of hard drives but not before it transferred the data back to the virus's source. This did not cause any physical damage but resulted in production delays and impacted business processes for almost two weeks. The virus was traced to a hacking group operating out of Iran, which referred to itself as “The Cutting Sword of Justice.” It is uncertain if the Iranian government sanctioned the attack, but in a country with controlled internet, they were definitely aware of it. An important “lesson’s learned” moment from this attack was the importance of keeping operations segregated into different and independent computer systems.

Europe & European Union

Policies and Initiatives

Bendiek, Annegret. "Europe’s Patchwork Approach to Cyber Defense Needs a Complete Overhaul." Council on Foreign Relations. August 30, 2017. https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul.

Despite extensive policies and agreements among the European Union, there is still doubt as to how the EU would react to a cyberattack targeting key critical infrastructure. One of the major problems lies in the decentralized cyber defense agencies that operate independently. In order to effectively combat significant cyber threats, the organizations would need to work in congress, something that has not yet been resolved. The article suggests that a comprehensive review and restructuring of the EU’s cyber defense policies, and an organizational shift from multiple decentralized agencies into a single centralized body would harden the EU’s ability to respond to cyber threats.

European Commission. European Union External Action. "EU Cybersecurity plan to protect open Internet and online freedom and opportunity." News release, February 7, 2013. European Commission. http://europa.eu/rapid/press-release_IP-13-94_en.htm.

This press release by the European Union outlines their cybersecurity strategy in an effort to protect European democracy and their digital economy. The policy must be adopted by each member state, and must adhere to security practice standards established by the EU. The EU's new strategy has five key priorities.

1. Achieve cyber resilience
2. Reduce cybercrime
3. Develop cyber defense policy and capabilities related to the Common Security and Defence Policy (CSDP)
4. Develop the industrial and technological resources for cybersecurity
5. Establish a coherent international cyberspace policy for the EU and promote EU values

United States

RELATIONSHIP WITH RUSSIA

McClintock, Bruce. "Respond to Russia's Information Warfare." US News & World Report. July 17, 2017. https://www.usnews.com/opinion/world-report/articles/2017-07-17/the-us-needs-a-response-to-russias-information-warfare.

This article outlines how the history of Russian information operations has molded their efforts in the modern cyber world. What was once traditional espionage is now launched through cyberspace, and the United States has found itself the target (sometimes indirectly) of those efforts. The United States now has to decide how to react and respond to Russian cyber-attacks, and one such method could be advancing the conversation on establishing normative behavior for state actors in cyberspace.

Libicki, Martin C. "Checklist for a U.S.-Russia Cyberwar." Tech Crunch. October 31, 2016. https://techcrunch.com/2016/10/31/checklist-for-a-u-s-russia-cyberwar/.

This article by Rand Senior Scientist Martin Libicki examines the fallout of the Russian election tampering and offers a question response format to some of the most provoking questions involving a cyberwar between Russia and the U.S. Some of the questions asked are, what type of response should the U.S. have for Russian aggression? How harsh should the response be? Which nation has greater capability to fight a cyberwar? Who would win in a tit-for-tat fight in cyberspace?

U.S. CAPABILITY

Paul, Christopher, and Rand Waltzman. "How the Pentagon Should Deter Cyber Attacks." Strategy Bridge. January 10, 2018. https://thestrategybridge.org/the-bridge/2018/1/10/how-the-pentagon-should-deter-cyber-attacks.

The Pentagon needs to realize that state actors and non-state actors alike are "not afraid to launch attacks against the United States in and through cyberspace." While they may not be willing to escalate to full conflict, cyberattacks which occupy a space in the grey zone are mediums which nations are willing to launch disruptive attacks that the Pentagon needs to be prepared to defend against. This article outlines five recommendations that the Pentagon can use to better defend themselves against cyber threats. First, the DoD should narrowly define the scope of how cyber is used and categorize cyber efforts appropriately. Second, expand the cyber domain into the physical domain so that cyber efforts have an impact on other capabilities and activities. Third, deterrence should be thought of as influence, and should focus on how actions are perceived internationally so that the U.S. response can change how potential aggressors make their decisions. Fourth, attempt to develop norms that can play a role in deterrence and establishing expected responses to behavior in the cyber domain. Fifth, establish consequences for adversarial actions that are appropriate.

U.S. Cybersecurity Strategy

Porche, Isaac R. III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1600.html. Also available in print form.

This report provides recommendations to the Army's Cyber Command for incorporating cyber operations into the Army's conventional warfighting capability. The Army's efforts to support their conventional warfighters with defensive and offensive cyber warfare is a delicate process that requires JIIM partners to be integrated at the tactical and strategic level without the Arm's ability to kinetically engage the enemy. The report highlights key challenges and recommendations to approach this daunting task.

United States. Department of Defense. Secretary of Defense. *The DoD Cyber Strategy.* April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

This document is the DoD Cyber Strategy that is implemented by all branches of the U.S. Military and its partners. As the focus continues to shift away from irregular warfare and towards state-to-state conflict, the cyber domain will become increasingly contested. This document outlines the DoD's doctrine and strategy for employing force and exerting influence across cyberspace.

U.S. Hegemony

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *The MIT Press*28, no. 1 (Summer 2003): 5-46.

https://www.belfercenter.org/publication/command-commons-military-foundation-us-hegemony.

This article emphasizes the preservation of U.S. hegemony through the application of military force and deterrence activities across multiple domains. U.S. dominance of common space (air and sea) preserves the power of the U.S. over other great powers, and this "command of the commons" is what allows for the U.S. and its allies to exert political influence beyond its borders. As we move forward into a new common, the cyber domain, the principles discussed in the exertion of command over the commons may prove valuable in preserving U.S. hegemony and deterring other great powers from challenging allied interests in contested spaces.

Cultural Coercion & Political Manipulation

RUSSIAN INFORMATION WARFARE

Giles, Keir. "Handbook of Russian Information Warfare." *NATO Defense College (NDC)*. Fellowship Monograph. November 9, 2016. http://www.ndc.nato.int/download/downloads.php?icode=506

This piece by the NDC provides a look at Russian information warfare from the start of the Russian invasion of Crimea in 2014 to 2016. Russia would not only utilize its own ideas and concept but borrow techniques and practices that it though other countries would using against it and in turn fold them into the Russian arsenal of information warfare. This guide seeks to provide an introduction to Russian information warfare along with its origins, evolution and potential future challenges. This style of warfare is not limited to pre-hostilities or active warfare but is a constant endeavor to gain the upper hand in any way possible. The techniques are not just limited to hacking and theft of information but coordinated campaigns by state sponsored media, government sources, celebrities and TV shows, online videos and widespread online trolling campaigns are all utilized to control opinions at home and garner support abroad.

RUSSIAN PROPAGANDA

Frenkel, Sheera. "Were You a Victim of Russian Propaganda? Facebook Will Help You Find Out." *New York Times*, November 22, 2017. https://www.nytimes.com/2017/11/22/technology/facebook-russia-propaganda.html

Utilizing fake posts and manufacturing news stories and groups, paid Russian propagandists posted information on Facebook on Instagram that was seen by over 29 million Americans and after sharing and re-sharing the posts, it is believed that 150 million people saw this post. The Russian government purchased ads directly from Facebook and an estimated 10 million people saw these ads on Election Day along. These posts were utilized to antagonize, influence and mislead users. Facebook, Twitter

and Google all were required to testify before Congress in regards to what they were doing to counter this.

Transportation Vulnerabilities

PRIVATE AND COMMERCIAL TRANSPORTATION

Curran, John. "Senators Reintroduce Bills Focused on Vehicle, Aircraft Cybersecurity." *Cybersecurity Policy Report* (March 27, 2017):1. http://search.proquest.com/docview/1884750619/FBA5175CE7A54BCAPQ/15?accountid=322

A bill was reintroduced to Congress with the goal of not only setting exact fines for specific hacking of cars and commercial aircraft but to require the U.S. manufacturers to install better hacking countermeasures. The bill also calls for isolation systems to prevent the entire vehicle from being impacted if hacked and will require a "cyber dashboard" which will show the consumer the level of hacking protection and privacy protection the vehicle has above the minimum set by the government. Also, any attempted or successful attacks would need to be shared with the manufacturers and the FAA in order to identify and fix the exploit.

Laws and Rulings/Treaties/Documentation

INTERNATIONAL ARMS CONTROL AGREEMENTS, NORMATIVE BEHAVIORS, POLICIES

Nye, Joseph S. "How Will New Cybersecurity Norms Develop?" Australian Strategic Policy Institute. March 12, 2018. https://www.aspistrategist.org.au/how-will-cybersecurity-norms-develop/.

In the United Nations, there is currently no regulatory body to protect citizens from cyber warfare. During a time when cyberattacks are among the greatest source of concern of international security, the international community is devoid of laws and norms that govern the environment. The internet is transnational, though the operators fall under sovereign nations. As the world becomes more networked, the potential targets for attack and number states and non-state actors able to commit cybercrimes will grow, requiring regulations to be created that administer over the cyber domain.

Herr, Trey. "Governing Proliferation in Cybersecurity." Global Summitry. July 3, 2017. https://academic.oup.com/globalsummitry/advance-article/doi/10.1093/global/gux006/3920644?guestAccessKey=f88e2727-737a-4be2-991e-a3696624b420.

This article compares international attempts to control the use of cyber weapons to WMD proliferation efforts. The article examines several different models of regulation and controls by looking at the use of proliferation, alliances, and proxy relationships, and determines their effectiveness in governing international cybersecurity initiatives.

Morgus, Robert. "Russia Gains an Upper Hand in the Cyber Norms Debate." Council on Foreign Relations. December 5, 2016. https://www.cfr.org/blog/russia-gains-upper-hand-cyber-norms-debate.

Following the Russian meddling in the U.S. democratic process, nations are now scrambling to create an established set of international norms on how states deal with attacks that occur over cyberspace. The article introduces two forms of normative behaviors in international politics, 'actual norms' where states understand expected behavior and mostly adhere to it, and 'aspirational norms' where states understand an expected behavior, but they are not institutionalized or universally accepted. The cyberspace debate falls into the latter category, and without international regulation and established institutional norms, influence operations and directed attacks over cyberspace will continue to be met with varying degrees of arbitrary response.

Nye, Joseph S. "The World Needs an Arms-control Treaty for Cybersecurity." Washington Post. October 1, 2015. https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html.

This article by Joseph Nye argues International cybersecurity requires an arms-control treaty. In modern history, devastating technologies that have the ability to change the landscape of battlefields have been met with arms-control agreements. Cybersecurity is the next such technology that requires international norms and treaties to govern its use. The author argues that the approaches of the past cannot be used as an effective model, as the static nuclear treaties do not translate well into an involving cyber world that exists in grey areas. Treaties that generate normative behavior must be the goal during the formation of cyber arms-control agreements.

Gerstein, Daniel M. "Define Acceptable Cyberspace Behavior." Rand. September 27, 2015. https://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html.

As China and the U.S. met in part to discuss cyberspace behavior and agree to terms that would prevent cyber espionage, their meeting fueled the debate over what is acceptable normative behavior. The article continues to discuss other international treaties and how a framework of defining cyberspace behavior that would be acceptable to all international parties may be problematic. The first step is to create a comprehensive cyber doctrine that defines how the U.S. responds to targeted cyber based offenses by state actors.

TALLINN MANUAL

Schmitt, Michael N., and Liis Vihul, eds. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Cambridge: Cambridge University Press, 2017.

This four part video series of the panels held at the symposium covers the topics of sovereignty in cyberspace, jurisdiction over cyber activities, international human rights laws in cyberspace and other topics. Featured panel speakers included representatives from USMA West Point, Harvard, Cornell, NATO CCD COE, UCLA, Syracuse University, University of Texas, Boston University, University College London, BYU Law School, Stifftung Wissenschaft und Politik, and Human Rights Watch.

STATE LEGISLATURE

National Conference of State Legislatures. "Cybersecurity Legislation 2016." December 8, 2016. http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx

This is an annually updated collection of state cybersecurity legislation and including a description and the status of each proposal.

AFRICAN INTERNET CONTROLS

Ellis, Harriet. "Freedom or Firewalls: Shaping Africa's Internet." International Institute for Strategic Studies. February 27, 2017. https://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2017-adeb/february-b85c/freedom-or-firewalls-c6ea.

Political stability and the disruptive power of social media are shaping how African nations are crafting policy and governing the internet. In Africa, while only 25% of the population use the internet, that number is rising quickly with the distribution of smartphones and other handheld devices. As nations like Cameroon begin to regulate internet usage in their country in a way that mirrors the Chinese model of controlled cyberspace, western democracies contest that the regulations can disrupt democratic processes and ideologies.

Ethics/Ambiguity

Singer, P.W. "Stuxnet and its Hidden Lessons on the Ethics of Cyberweapons." *Case Western Reserve Journal of International Law* 47 (2015): 79-86. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1009&context=jil

This article briefly describes the use of the Stuxnet worm and its end goal before moving on to evaluating the ethics of utilizing this particular cyberweapon and cyberweapons in general. While Stuxnet might be seen as the digital "Pandora's Box" for state sponsored cyberattacks, the worm itself only impacted one particular system and did not harm any of the other devices it infected in order to transmit itself to the final target of Iranian

nuclear centrifuges. This worm was unique in that a digitally transmitted action caused real-world physical destruction yet had no collateral damage or caused any physical harm to individuals working at the facility.

Crosston, Matthew. "DUQU's DILEMMA: The Ambiguity Assertion and the Futility of Sanitized Cyber War." *Proceedings of the International conference on Information Warfare & Security*. (January 1, 2013):43-50. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=86139890&site=ehost-live

In order to attempt to discern an appropriate state level response to cyberattacks, regulators and international orders repeatedly call for the Law of Armed Conflict or a form of internationally adopted legal framework to be utilized/created to create a standardized response to a cyberattack. However, cyberattacks blur the lines between military and civilian, often time using civilian systems in order to protect the sponsor state's government from retribution. These standards, normally applied to physical conflict are not enforceable nor applicable to the ambiguity of the cyber realm.

National/International Cybersecurity

CENTERS/AGENCIES & POLICIES

"Organizations and Institutions That Address International Cybersecurity." Information Technology Industry Council. https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf.

This document by the Information Technology Industry Council is a comprehensive list of every known organization and institution that addresses international cybersecurity and provides a link to the organization's website, and the scope of their operations.

U.S. Cyber Command (USCYBERCOM). http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

U.S. Cyber Command leads the daily operations required to protect the Department of Defense networks from intrusion, outside attacks and any from being compromised in anyway. It also conducts military cyberspace operations and supplies support for external missions and increases the U.S.' ability to withstand cyberattacks. USCYBERCOM includes the cyber commands for all of the armed forces and its own Cyber Missions Teams.

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). https://ccdcoe.org/

This NATO center is a compilation of experts from various backgrounds, including, educators, military, government, researchers and analysis with the purpose of providing a thorough look at current levels of cybersecurity and who to improve upon them. This center consists of members from 20 different nations.

Educational Resources/Tools/Contextualizing Cyber

EDUCATIONAL RESOURCES AND TOOLS

International Cyber Developments Review (INCYDER). NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). https://ccdcoe.org/incyder.html

The INCYDER is NATO's interactive research database for legal and policy documents that are utilized by international cybersecurity organizations. The database is periodically updated to reflect institutional changes to international cybersecurity regulations and policy.

Mcroskey, Erick D., and Charles A. Mock. "Operational Graphics for Cyberspace." *Joint Force Quarterly* 85 (2nd Quarter, April 2017): 42-49. http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-85/Article/1130660/operational-graphics-for-cyberspace/

This article utilizes graphical representation, common in military briefings, to depict cyberdefense and a simulated cyberattack. The use of familiar graphics and a descriptive layout allows for easier comprehension of an oftentimes difficult topic. The article begins by explaining why it uses certain graphic and how some had to be slightly altered to accurately depict aspects of cyber defense. The graphics included show a common layout of a network and how it is managed and protected, followed by notational cyber unit icons, notational cyberspace terrain, and the sequential actions of multi-layered cyberattack. It concludes with showing how mission graphics can be adopted into the cyber realm and a final graphical depiction of how an adversary can steal legitimate credentials and infiltrate a secure network.

National Institute for Cybersecurity Careers and Studies. Department of Homeland Security. https://niccs.us-cert.gov/training

This official DHS site provides free directed and independent study online courses and in-classroom training in cybersecurity for government employees, government contractors, veterans, and in a more limited capacity to state, local and tribal employees/officials. The majority of the coursework is designed for career training yet there are several courses that serve to bring a greater understanding of cybersecurity and cyber-threats.

United States Computer Emergency Readiness Team (US-CERT) https://www.us-cert.gov/.

The US-CERT was established in 2003 following several Federal Government cyber breaches in 2000. The agency's mission is to:

- Provide cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities
- Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
- Responding to incidents and analyzing data about emerging cyber threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

CONTEXTUALIZING CYBER

"Cyber Analogies." Naval Post Graduate School. February 28, 2014. https://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf.

The challenges faced in the cyber domain are new to policy makers and strategists alike. By creating analogies for cyber related events with well-known events in military history, a contextual framework is established to reduce the complexity of the challenges faced in the cyber domain. The report's goal is to ground cyber challenges in reality for those without expertise.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security*38, no. 2 (Fall 2013): 41-73. https://www.belfercenter.org/publication/myth-cyberwar-bringing-war-cyberspace-back-down-earth.

Cyber is the newest domain that world powers are jockeying over for control. A weapon that almost exclusively is used against sovereign states as opposed to the kinetic weaponry used in the proxy wars fought against third parties. Cyber systems support all aspects of modern warfighting and state infrastructure activities in most nations, and the employment of offensive cyber capabilities can cripple multiple facets of a nation's ability to conduct military operations without attribution. The article aims to ground cyberwar as a contemporary strategy for military strategists to achieve tactical objectives. Cyber capabilities merely enhance the toolkit of strategists so that they can more effectively inflict damage on adversaries in a multitude of ways.

Ferdinand, Jason. "Building Organisational Cyber Resilience: A Strategic Knowledge-Based View of Cyber Security Management." *Journal of Business Continuity & Emergency Planning* 9, no. 2 (September, 2015):185-195. https://www.ncbi.nlm.nih.gov/pubmed/26642176.

This publication analyzes cyber resilience in an increasingly cyber dependent world and makes recommendations as to how an organization can build a program that maintains and assesses its cyber resilience.