Center on Sanctions
& Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Resource Document

Framework and Terminology for Understanding Cyber-Enabled Economic Warfare

Samantha F. Ravich, Ph.D., Principal Investigator

Annie Fixler, Policy Analyst

February 22, 2017

Foreword

The world is witnessing a new kind of war, fought not with bullets but with banknotes and bytes. Although the use of economic aggression against an adversary traces nearly as far back as the creation of economic systems – economic success can breed economic competition which in turn can become intertwined with adversarial relations – over time, economic warfare tactics have evolved. Today, the arsenal consists of many long-established techniques as well as new, innovative tools (some legal and some not) reflective of our modern economic and financial systems. But now the battleground is shifting faster. The expanding digital landscape is changing the nature of economic warfare. Something new is developing: cyber attacks and cyber-enabled attacks can now cause economic harm disproportionate to the size or resources of the attacker.

While traditional economic warfare and cyber warfare have both been extensively studied, the intersection between these two subjects has not received the consideration it warrants. Greater focus, comprehensive study, and policy attention is needed to understand the evolution of economic warfare within the new realities of cyber space. With the rise of the global, networked economy and the integration and interdependence of its constituent parts, nation states and criminal organizations alike are expanding opportunities to develop new methods and strategies of economic warfare. Both states and non-state actors are increasingly able to contemplate and deploy pernicious cyber attacks against the critical economic assets and systems of their adversaries, targeting their national security and military capabilities. This new class of threats is "cyber-enabled economic warfare" (CEEW).

The United States needs new doctrines, analytic and collection tools, and strategies to ensure we can advance our national security interests in this changing landscape. But before these can be produced, we must first develop a common language to understand the nature of the cyber threats the United States and its allies face. Too often, ambiguity, disagreement, or a lack of clarity over terminology hinders Washington's ability to work with its allies, engage the private sector, and communicate with the American people about challenges and opportunities in cyber space. This paper, and the broader project that underlies it, aims to address this shortcoming by offering a coherent set of definitions of different types of cyber attacks. It also serves as the beginning of a conversation about how we understand the myriad threats we face so that we can develop effective policies to defend against them.

To supplement and add texture to the definitions, this paper also provides examples of various types of cyber attacks that have occurred over the past decade. These classifications illuminate how government officials and private sector practitioners can better understand the intentions of their adversaries.

Cyber-enabled economic warfare may pose one of the most significant and misunderstood threats to U.S. national interests over the next decade. It is critical that policymakers across the political spectrum begin a robust effort to comprehend this evolving battle space so as to prevail within it.

We are pleased to serve as advisors to the Cyber-Enabled Economic Warfare project at the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance.[1]

Stewart Baker
John P. Carlin
Steven Chabinsky
Frank Cilluffo
Rajesh De
Mark Dubowitz
Karen Evans
Nick Fishwick CMG
Gen. Michael V. Hayden
Todd Hinnen
Michael Hsieh
Jamil Jaffer
Jeffrey Johnson
Herbert Lin
Chip Poncy
David Shedd
Rhea Siers
Matthew Spence
V.S. Subrahmanian
Mark Weatherford
Juan C. Zarate

Introduction

There is no common lexicon within the U.S. government, between the public and private sector, and among Washington and its allies to describe cyber incidents – be they cyber espionage, cyber sabotage, or cyber warfare. The NATO Cooperative Cyber Defence Centre of Excellence, for example, lists 15 different definitions from member and non-member countries for the term "cyber attack" and 11 definitions for the term "cyber terrorism."[2] A lack of common language impedes a government's ability to communicate with its citizens and to craft timely, cohesive policies, especially when confronted with an attack.[3]

FDD's Cyber-Enabled Economic Warfare project was established to put an analytic and policy framework around a specific type of malicious cyber activity that is occurring but is going relatively unnoticed. These are attacks against a nation wielding cyber technology with the *specific intent* to weaken its economy and thereby undermine its political and military power. The key is recognizing the adversarial strategy that underpins it. Through such a framework, seemingly unconnected hostile cyber actions (e.g. cyber crime, cyber espionage, or cyber terrorism) can be better understood, giving insight into the broader campaign plan and suggesting means to thwart, defend against, or ultimately deter it. To aid in this endeavor, this project has researched existing understandings and

[1] For more information on the project's senior advisory group, visit: http://www.defenddemocracy.org/ceew-advisory-members

[2] NATO Cooperative Cyber Defence Centre of Excellence, "Resources: Cyber Definitions," accessed October 17, 2016. (https://ccdcoe.org/cyber-definitions.html)

[3] For example, after the Australian Bureau of Statistics (ABS) suffered a DDoS (distributed denial of service) attack in 2016, media reports initially called the incident a "hack." ABS head statistician David Kalisch then clarified that it was not a hack but rather an attack because hacks are attempts to steal information, and this attack only took down the census website. Appearing alongside Kalisch, however, MP and Small Business Minister Michael McCormack denied that the incident was either a hack or an attack, but rather "an attempt to frustrate the collection of data." Special Advisor to the Prime Minister on Cyber Security Alastair MacGibbon also called the incident an attack, but tweeted that it was "not a hack, a breach or a compromise, it's an inconvenience." These competing statements focus the debate on definitions rather than appropriate responses and, more importantly, do not address the potential long-term effect of the incident: the loss of public trust in government institutions.

selected the following terms and definitions in order to create a unified understanding of the framework in which states and non-state actors operate. We recognize that these terms and definitions may need to be revised over time as both our understanding and the environment itself likely will change.

We recommend that the U.S. government consider adopting these definitions.

Definitions

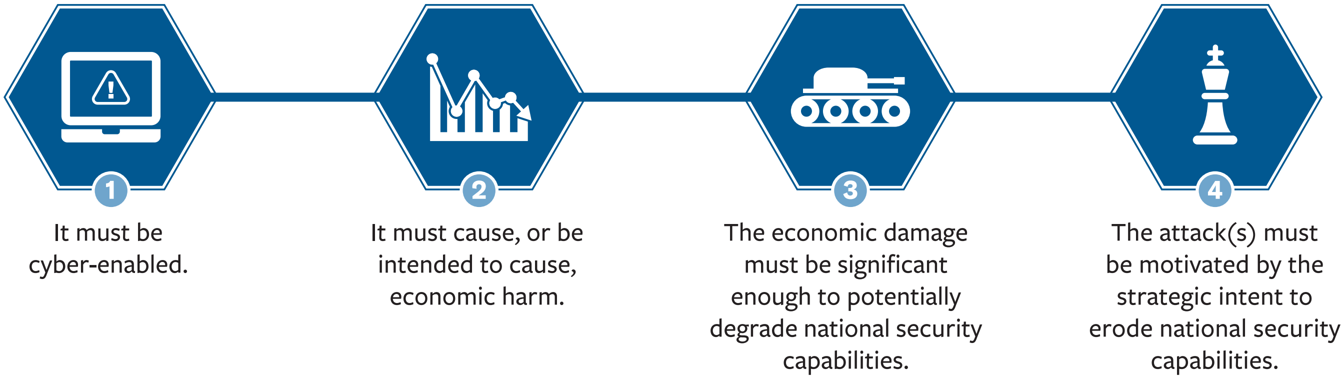
Cyber-enabled economic warfare (CEEW)

Refers to a hostile strategy involving attack(s) against a nation using cyber technology with the intent to weaken its economy and thereby reduce its political and military power.[4]

The term cyber-enabled economic warfare identifies the evolving dynamic in which technological developments are facilitating state and non-state actors' ability to engage in new economic warfare strategies.

To determine if an attack is part of a CEEW campaign, it is necessary to understand the strategic intent of the attacker. While an individual attack might be classified as cyber crime or cyber espionage, the broader context and strategy of the attacker must be understood in order to craft appropriate counter-strategies.

An attack, or collection of attacks, constitutes CEEW if it meets the following four requirements:



1. It must be cyber-enabled.
2. It must cause, or be intended to cause, economic harm.
3. The economic damage must be significant enough to potentially degrade national security capabilities.
4. The attack(s) must be motivated by the strategic intent to erode national security capabilities.

A subcategory of CEEW is cyber financial warfare. These attacks are purposely intended to degrade, compromise, or undermine the infrastructure, data, functioning, and faith in the financial system and its relevant institutions as a means to degrade the political and military power of an adversary.[5]

[4] Samantha Ravich, "Cyber Enabled Economic Warfare: An Evolving Challenge (Vol. 2)," *The Hudson Institute*, November 2015, page 29. (https://s3.amazonaws.com/media.hudson.org/files/publications/20151117RavichCyberEnabledEconomicWarfareAnEvolvingChallengeVol2.pdf)

[5] Juan Zarate, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," *Foundation for Defense of Democracies*, June 2015. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf)

Cyber crime

Involves 1) the unauthorized access of a network in order to steal, destroy, or otherwise alter information, commit fraud or extortion, or damage property (physically or virtually), or 2) the denial of access to a network by rightful users.[6] When employed in service of achieving the broader strategic goal of undermining the economic viability of a nation state in order to damage its national security capacity, the cyber crime itself becomes a tactic within a cyber-enabled economic war plan.

Cyber crime is a broad category that includes activities that can also be classified as cyber espionage or cyber terrorism. The primary difference between a cyber attack to commit a crime or to launch a terrorist attack or to wage a cyber-enabled economic warfare campaign is found in the intent of the attacker.[7]

Law enforcement agencies have no universal definition of cyber crime.[8] The Budapest Convention on Cybercrime of 2001, ratified by 49 nations,[9] does not include a singular definition of cyber crime, but rather outlines a series of actions that nation states should take to protect against certain types of criminal activity.[10]

Under our definition, the global cost of cyber crime has expanded exponentially over the past five years and may reach as high at $2 trillion annually by 2019, according to some experts.[11]

[6] This definition is based on the statute on fraud and related activity in connection with computers. 18 U.S.C. §1030: Fraud and related activity in connection with computers. (https://www.law.cornell.edu/uscode/text/18/1030)

[7] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," *Congressional Research Service*, January 29, 2008. (http://www.fas.org/sgp/crs/terror/RL32114.pdf)

[8] Interpol, "Cybercrime," accessed October 19, 2016. (https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime); For a list of definitions, see NATO Cooperative Cyber Defence Centre of Excellence, "Resources: Cyber Definitions," accessed October 17, 2016. (https://ccdcoe.org/cyber-definitions.html)

[9] Council of Europe, "Chart of signatures and ratifications of Treaty 185," October 19, 2016. (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures)

[10] Council of Europe's Convention on Cybercrime, Budapest, November 23, 2001. (http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561)

[11] "Cybercrime Will Cost Businesses Over $2 Trillion by 2019," *Juniper Research*, May 12, 2015. (https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion)

Cyber deterrence

Is the manipulation of an adversary's cost/benefit analysis of a given cyber activity.[12] A nation can convince its adversary to avoid taking a specific action by reducing the prospective benefits and/or increasing the prospective costs.[13]

According to the U.S. Department of Defense, cyber deterrence is built from a combination of "declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems."[14] Deterrence works by convincing an adversary that its actions will not succeed and that it will suffer significant consequences.[15]

Unlike the nuclear era, it is now possible to defend or mitigate the effects of a cyber attack. However, deterrence will need to focus on shaping targeted actors' behavior and deterring actions (individually or as part of a larger campaign) above a certain threshold, rather than preventing all forms of cyber attacks, which is impossible.

Given the challenges of attribution inherent in cyber space, it is particularly important in cyber deterrence for targeted adversaries and third-parties to recognize when a counter-action to dissuade, mitigate, combat, or punish an action has been taken. However, an effective counter-measure to a cyber attack may not necessarily require a parallel cyber action in return.

There is also much discussion about how models of deterrence might be applied in a battle space where states do not hold a monopoly of power. The private sector plays a large role in cyber defense – again, unlike during the nuclear era – and yet there remain significant legal questions about what private companies are permitted to do, especially with regards to active defense.[16] A "cyber privateering" model may also provide an innovative way to create deterrence by leveraging a broad array of actors.[17] As policymakers craft strategies of cyber deterrence, robust engagement with the private sector is critical.

[12] "Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity," Eds. James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher, and Valery Yaschenko, *East-West Institute*, February 2014, page 51. (https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf)

[13] The definition of deterrence is adapted from Austin Long, "Deterrence: From Cold War to Long War," *RAND Corporation*, 2008, page 7. (http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG636.pdf)

[14] Consistent with the Pentagon's usage, we define cyber deterrence as the deterrence of cyber activities. According to the Defense Department, a "comprehensive cyber deterrence strategy… deter[s] key state and non-state actors from conducting cyber attacks against U.S. interests." In contrast, we define the term cyber-enabled deterrence to mean the use of cyber means to deter a range of adversarial activities including but not limited to cyber-enabled economic warfare. Cyber-enabled deterrence is the exclusive use of cyber means to deter an enemy's action inside or out of the cyber realm. U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 2015, pages 10-11. (http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

[15] Ibid.

[16] "Into the Gray Zone The Private Sector and Active Defense Against Cyber Threats," *Center for Cyber and Homeland Security, The George Washington University*, October 2016. (https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf)

[17] Juan Zarate, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," *Foundation for Defense of Democracies*, June 2015, pages 20-27. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf)

Cyber espionage

Refers to the gathering and/or transmitting of information relevant to national security; the gathering or delivering of national security information to aid foreign governments; and the disclosure or communication of classified information using or facilitated by a cyber operation.[18] Cyber espionage includes attacks against both governments and private companies. When employed in service of achieving the broader strategic goal of undermining the economic viability of a nation state to damage its national security capacity, cyber espionage itself becomes a tactic within a cyber-enabled economic war plan.

This definition departs from the more traditional definition of espionage, which differentiates between national security and commercial interests. Through the wider lens of CEEW, and recognizing that U.S. adversaries do not draw such a distinction, the understanding of cyber espionage must be modified.

Technological advancements have changed the methods but not the intentions behind nation-state espionage, and the relevant national and international laws are well established. According to the Department of Justice, existing espionage laws "provide solid grounds for prosecution." Additionally, the Computer Fraud and Abuse Act provides additional authorities if a person "without authorization or in excess of authorized access, deliberately accesses a computer, obtains national security information, and seeks to transmit or communicate that information to any prohibited person."[19]

U.S. adversaries and competitors use cyber espionage to steal intellectual property and undermine the global competitiveness of U.S. companies.[20] The intention of a cyber attack against a commercial interest may be solely to gain market share; however, it may also be to undermine the nation's economic foundation and erode national security capabilities. Indeed, cyber espionage against commercial interests can affect not only the economic performance of a country but also its ability to defend itself and project power.

[18] This definition is adapted from the U.S. legal code's definition of espionage, "Espionage and Censorship," 18 U.S.C. §791-799. (https://www.law.cornell.edu/uscode/text/18/part-I/chapter-37) as well as *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, Eds. David Clark, Thomas Berson, and Herbert S. Lin, (Washington, DC: The National Academies Press, 2014), Chapter 1, page 14. (http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-20150303-SD006.pdf); For alternative definitions, see NATO Cooperative Cyber Defence Centre of Excellence, "Resources: Cyber Definitions," accessed October 17, 2016. (https://ccdcoe.org/cyber-definitions.html); "Cyber Espionage," *Financial Times Lexicon* (UK), accessed October 19, 2016. (http://lexicon.ft.com/Term?term=cyber-espionage)

[19] U.S. Department of Justice, Office of Legal Education, "Prosecuting Computer Crimes," January 14, 2015, page 15. (https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf)

[20] "America's Cyber Future: Security and Prosperity in the Information Age," Eds. Kristin M. Lord and Travis Sharp, *Center for a New American Security*, June 2011, page 13. (https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf)

Cyber sabotage

Is a deliberate, malicious cyber-enabled act that disrupts normal network processes or functions, or that destroys or damages equipment or information.[21] When employed in service of achieving the broader strategic goal of undermining the economic viability of a nation state to damage its national security capacity, cyber sabotage itself becomes a tactic within a cyber-enabled economic war plan.

Cyber sabotage motivated by financial interests is a form of cyber crime, while attacks intended to affect government decisions should be classified as cyber terrorism. Cyber sabotage describes the type of damage resulting from an attack as well as the means for it, rather than the motivation behind the incident.

Cyber terrorism

Is the criminal use of information technology to cause severe disruption or harm in order to influence the conduct of a government or private institution by intimidation or coercion, or to retaliate against government conduct.[22] When employed in service of achieving the broader strategic goal of undermining the economic viability of a nation state in order to damage its national security capacity, cyber terrorism becomes a tactic within a cyber-enabled economic war plan.

Under U.S. law, the prevailing definition of terrorism is an act that "is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct" and violates one or more of a series of laws, including those related to destruction of aircraft, weapons of mass destruction, arson and destruction of property, hostage taking, destruction of communication systems, among many others.[23] In 2001, Congress used the USA PATRIOT Act to expand the definition of terrorism to include crimes related to computers under 18 U.S. Code §1030.[24] In short, violations of the Computer Fraud and Abuse Act can be defined as cyber espionage, but if those activities are for the purpose of affecting government policy, they can also be defined as terrorism.

[21] Definition adapted from Kevin Coleman, "Cyber Sabotage," *DefenseTech*, February 6, 2008. (http://www.defensetech.org/2008/02/06/cyber-sabotage/)

[22] This definition is adapted from the U.S. legal code's definition of terrorism, and from the Oxford English Dictionary: "The politically motivated use of computers or information technology to cause severe disruption or widespread fear." "Cyberterrorism," *English Oxford Living Dictionaries*, accessed February 16, 2017. (https://en.oxforddictionaries.com/definition/cyberterrorism)

[23] Federal Bureau of Investigation, "What We Investigate: Terrorism," accessed December 21, 2016. (https://www.fbi.gov/investigate/terrorism)

[24] U.S. Department of Justice, Office of Legal Education, "Prosecuting Computer Crimes," January 14, 2015, page 15. (https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf); 18 U.S.C. §1030: Fraud and related activity in connection with computers. (https://www.law.cornell.edu/uscode/text/18/1030); 18 U.S.C. §2332b: Acts of terrorism transcending national boundaries. (https://www.law.cornell.edu/uscode/text/18/2332b)

Terrorist groups increasingly use cutting-edge technology to recruit, fundraise, distribute propaganda, and conduct attacks. These groups understand that Western economic, cultural, and political dependence on cyber space presents a vulnerability that can be exploited.[25]

Cyber terrorism is most often defined as an unlawful attack(s) or threat(s) of an attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.[26] However, we believe that it is more useful for national security purposes to look at the tools and techniques of the *attacker* (cyber means) rather than the target *attacked* (cyber domain).

Cyber warfare

Is a conflict conducted by cyber means, in whole or in part. Acts of cyber warfare are aimed at degrading an adversary's military capabilities or denying an adversary the effective use of its cyber systems and weapons.[27] Cyber warfare is distinct from cyber-enabled economic warfare because the former is focused on directly degrading military capabilities while the latter is intended to cause economic harm as a way to indirectly degrade national security capabilities.

Definitions of cyber warfare are often so broad as to encompass everything from cyber terrorism to cyber-enabled economic warfare.[28] FDD's Cyber-Enabled Economic Warfare project uses the term as defined above by the Joint Chiefs of Staff.

[25] Canada's Cyber Security Strategy For A Stronger and More Prosperous Canada, 2010, page 5, as quoted in Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions," *New America*, October 2014, page 59. (http://giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf)

[26] Dorothy E. Denning, "Cyberterrorism," *Testimony before the House Armed Services Committee, Special Oversight Panel on Terrorism*, May 23, 2000, page 1. (http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf); Similarly, the Federal Emergency Management Agency defines cyber terrorism as "Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives," as quoted in Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," *Congressional Research Service*, January 29, 2008, page 4. (http://www.fas.org/sgp/crs/terror/RL32114.pdf)

[27] This definition is adapted from that of the Joint Chiefs of Staff as outlined in Vice Chairman of the Joint Chiefs of Staff, "Joint Terminology for Cyberspace Operations," *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates*, November 2010, page 8. (http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf); For a list of alternative definitions, see NATO Cooperative Cyber Defence Centre of Excellence, "Resources: Cyber Definitions," accessed October 17, 2016. (https://ccdcoe.org/cyber-definitions.html)

[28] "Cyber Warfare," *RAND Corporation*, accessed October 20, 2016. (http://www.rand.org/topics/cyber-warfare.html)

Economic warfare

Entails the use of non-kinetic actions against an adversary's vital economic targets to weaken it economically and thereby reduce its political and military power.[29] It implies a substantial disturbance of the target's economy.

Economic warfare has been a part of societal conflict for millennia and has in the past included everything from sanctions and blockades to voluntary boycotts by citizens against another state.[30] Over the past decade and a half, the U.S. Department of the Treasury has been at the forefront of developing new financial tools to undermine the economies of adversaries and rogue actors. These new "smart sanctions" are structured to affect the leadership of a country or the individuals and companies involved in illicit activity, and cause less collateral damage than trade embargos and blockades. While the U.S. government regularly and aggressively uses these tools, it shies away from the term "economic warfare."

Economic warfare is distinct from traditional warfare (although it may be part of a larger military campaign) because it uses non-kinetic methods to target an adversary's economic resources rather than its military resources.[31] Cyber-enabled economic warfare is merely a new form of economic warfare, facilitated by emerging technology.

Cyber-enabled information warfare

Uses cyber means to influence the decisions or actions of a foreign nation by affecting the opinions, emotions, or attitudes of its citizens.[32] When employed in service of achieving the broader strategic goal of undermining a nation state to damage its national security capacity, cyber-enabled information warfare itself becomes a tactic within the execution of a larger war plan.

The term "information warfare" has been used in common parlance to describe non-kinetic attacks using information systems,[33] but the term "cyber warfare" has become more popular as an all-encompassing term. Similarly, the term

[29] This is based on the definition of economic warfare from George Shambaugh, "Economic warfare," *Encyclopedia Britannica*, accessed November 3, 2016. (https://www.britannica.com/topic/economic-warfare)
[30] Vaughan Lowe and Antonios Tzanakopoulos, "Economic Warfare," *Max Planck Encyclopedia of Public International Law*, Ed. Rüdiger Wolfrum, (Oxford University Press, 2012). (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701590)
[31] Tor Egil Førland, "The History of Economic Warfare: International Law, Effectiveness, Strategies," *Journal of Peace Research*, May 1993, page 151. (https://www.jstor.org/stable/425196?seq=1#page_scan_tab_contents)
[32] This definition is adapted from the Joint Chief's definition of military information support operations. U.S. Joint Chiefs of Staff, "Military Information Support Operations," January 7, 2010 incorporating change 1 December 20, 2011, page vii. (http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf)
[33] NATO Cooperative Cyber Defence Centre of Excellence, "Resources: Cyber Definitions," accessed October 17, 2016. (https://ccdcoe.org/cyber-definitions.html); Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions," *New America*, October 2014, pages 63-64. (http://giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf)

"electronic warfare" commonly refers to the use of radio signals or other electromagnetic signals to degrade an adversary's military capabilities. A more precise definition of "information warfare," as outlined above, is based on the defense community's definition of military information support operations, psychological operations, or influence operations.[34]

More than two decades ago, scholar Martin Libicki observed that there are seven distinct forms of information warfare: 1) command-and-control warfare, 2) intelligence-based warfare, 3) electronic warfare, 4) psychological operations, 5) "hacker" warfare (attacks on computer systems), 6) economic information warfare (using information to pursue economic dominance), and 7) cyber warfare (futuristic scenarios).[35] Information warfare can defeat or neutralize hostile military units by distorting, degrading, or capturing the adversary's battlefield knowledge infrastructure.[36] It can also be used to undermine another state's political and social systems or to psychologically manipulate an adversary's civilian population in order to sway a populace in a desired political direction.[37]

Real World Examples of CEEW and other Types of Cyber Attacks

An attack, or collection of attacks, constitutes cyber-enabled economic warfare (CEEW) if it meets the following four requirements:

- It must be cyber-enabled.
- It must cause, or be intended to cause, economic harm.
- The economic damage must be substantial – significant enough to potentially degrade national security capabilities.
- The attack (or series of attacks) must be motivated by strategic intent: to erode national security capabilities and reduce national political and military power.

The following examples outline attacks that are instances of: 1) cyber-enabled economic warfare; 2) cyber attacks that do not fit the CEEW criteria; and 3) attacks that may be part of a cyber-enabled economic warfare campaign but more information is needed to make a determination.

I. CEEW Attacks

Chinese theft of intellectual property: Beginning as early as the 1970s, China has been engaged in a massive, prolonged campaign of intellectual property theft against U.S. firms.[38] Over time, China has increasingly conducted these campaigns via cyber-enabled technologies, targeting nearly every sector of the U.S. economy

[34] The RAND Corporation uses a similar definition of an influence operation, see Eric V. Larson, et al, "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," *RAND Corporation*, 2009, page 2. (http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf)

[35] Martin C. Libicki, *What is Information Warfare?* (Washington, DC: Center for Advanced Concepts and Technology, National Defense University, 1995), page x.

[36] Richard B. Gasparre, "The Israeli 'E-tack' on Syria – Part I," *Airforce-Technology.com*, March 10, 2008. (http://www.airforce-technology.com/features/feature1625/)

[37] Russian Submission to the United Nations General Assembly Resolution A/54/213, 10 as quoted in Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions," *New America*, October 2014, page 63. (http://giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf)

[38] Christopher Cox, "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," *U.S. House of Representatives*, May 1999. (https://www.congress.gov/105/crpt/hrpt851/CRPT-105hrpt851.pdf)

and annually costing U.S. companies hundreds of billions of dollars and more than two million jobs.[39] China's intellectual property theft campaign constitutes a large, if not the largest, part of Beijing's overall CEEW strategy against the U.S. and the West. Washington and its allies have been slow to comprehend the threat, primarily because they view each attack individually as a separate incident instead of collectively as elements in an overall coordinated campaign. For example, in May 2014, the Department of Justice charged five Chinese hackers who targeted American companies in the nuclear power, metals, and solar industries with only computer crimes and espionage.[40] Similarly, accusations against China for theft of U.S. Steel's proprietary information only claim that Beijing is focused on market share,[41] without understanding how this fits a larger pattern.

Russian attacks on Estonia: In the spring of 2007, Russia sponsored (and likely orchestrated) concentrated cyber attacks (primarily distributed denial of service attacks) against Estonia.[42] The attacks took down government websites and hampered the ability of the government to communicate with its citizens. News organizations were affected and, finally, the attacks forced Hansabank, Estonia's largest bank, to cease all operations temporarily, nearly bringing the financial system to collapse. While ostensibly the catalyst was Russian anger over the Estonian government's relocation of a World War II memorial, Russia's true intent seems to have been to weaken the Estonian government and affect its policy decisions – a textbook case of cyber-enabled economic warfare.

Saudi Aramco attack: In mid-2012, Iran conducted a large-scale cyber attack against Saudi Aramco that destroyed 35,000 (three-quarters) of its computers and forced the company to revert to analog systems to communicate and manage contracts and supplies.[43] The massive cyber effort was part of a long-standing rivalry between the two countries and likely had multiple intended outcomes. These include not only damaging a major global oil competitor and driving up oil prices, but also harming Saudi Arabia's economy in order to erode Saudi support for economic sanctions against Iran for its illicit nuclear program. This cyber-enabled economic warfare campaign may also have been retaliation for an attempted attack on Iran's oil production systems in early 2012.[44] In recent years, Iran's cyber capabilities and willingness to cause physical damage appears to have expanded greatly, with some experts saying that Tehran has joined the "cyber superpower club."[45]

[39] Lesley Stahl, "The Great Brain Robbery," *60 Minutes, CBS News*, January 17, 2016. (http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/); "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research*, 2013. (http://www.ipcommission.org/report/ip_commission_report_052213.pdf)

[40] U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

[41] John W. Miller, "U.S. Steel Accuses China of Hacking," *The Wall Street Journal*, April 28, 2016. (http://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201)

[42] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian* (UK), May 16, 2007. (https://www.theguardian.com/world/2007/may/17/topstories3.russia)

[43] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012. (http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0); Jose Pagliery, "The inside story of the biggest hack in history," *CNN*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)

[44] Thomas Erdbrink "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet," *The New York Times*, April 23, 2012. (http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html); Jen Alic, "Attack on Iran's Oil Industry Ups Cyber Warfare Stakes," *Oilprice.com*, May 1, 2012. (http://oilprice.com/Energy/Crude-Oil/Attack-on-Irans-Oil-Industry-Ups-Cyber-Warfare-Stakes.html)

[45] Sam Jones, "Cyber warfare: Iran opens a new front," *The Financial Times* (UK), April 26, 2016. (https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3)

North Korean attacks on South Korea: For at least four years, Pyongyang has been conducting diversified cyber attacks on many parts of South Korea's infrastructure and economy. In March 2013, North Korean hackers attacked South Korean banks and media companies using malware dubbed "DarkSeoul," destroying tens of thousands of computers, deleting data from hard drives, overwriting bank records, and rendering many banking services inoperable.[46] Experts warn that North Korea may have learned the tactics and methodology from earlier attacks on Iran's nuclear and oil infrastructure apparently by the U.S. and Israel.[47] North Korea's intentions in the March 2013 attacks were not purely economic or commercial – that is, Pyongyang was not interested in advantaging its own media companies and financial institutions within the South Korean market by taking out their competitors. Rather, North Korea has engaged in a campaign of attacks designed to disrupt elements of the South Korean economy and to improve its own attack capabilities in order to develop the ability eventually to undercut South Korea's defense capabilities.

U.S. SWIFT-enabled sanctions regime on Iran: Beginning in 2006, U.S. financial sanctions on Iran for its illicit nuclear program and support for terrorism took on new dimensions and escalated dramatically until negotiations commenced between Iran and the international community in 2013. The U.S. sanctions regime took on a "cyber-enabled" element in early 2012 when Congress launched efforts to remove Iranian banks from the SWIFT international financial messaging network, which is a cyber-enabled system that serves as the backbone of the global financial system. The removal of Iranian banks was intended both to prevent illicit financial activities and to cause substantial harm to Iran's economy, and thereby pressure Iran to either change its policies or suffer degradation of funding for its military capabilities and support for terrorism.[48] Accordingly, although a somewhat unconventional case, the U.S. sanctions regime constitutes an example of CEEW.

II. Non-CEEW Attacks

The following examples are organized by category, (e.g. cyber crime, cyber espionage, cyber-enabled information war, cyber sabotage, and cyber terrorism).

Cyber Crime

GameOver Zeus botnet: In June 2014, the FBI and Department of Justice announced that a multinational effort disrupted a sophisticated malware known as the GameOver Zeus botnet.[49] The malware reportedly caused the theft of millions of dollars from U.S. and global companies and consumers by stealing user banking credentials and then initiating wire transfers to accounts controlled by the criminals. The Department of Justice indicted Russian citizen Evgeniy Bogachev as the head of the criminal gang responsible for the cyber crime operation.

[46] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *The New York Times*, March 20, 2013. (http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html); K.J. Kwon, "Smoking gun: South Korea uncovers northern rival's hacking codes," *CNN*, April 22, 2015. (http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/); "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," *Semantec Security Response*, June 26, 2013. (https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war)

[47] Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks," *Wired*, February 10, 2015. (https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/)

[48] Mark Dubowitz and Annie Fixler, "'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses," *Foundation for Defense of Democracies*, July 2015. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Enabled_Swift.pdf)

[49] Federal Bureau of Investigation, "GameOver Zeus Botnet Disrupted," June 2, 2014. (https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted)

Bangladesh central bank heist: Over one weekend in February 2016, criminals sent a series of fraudulent requests to the New York Federal Reserve to transfer $1 billion from an account belonging to Bangladesh to private accounts in Sri Lanka and the Philippines. The thieves infiltrated the Bangladeshi central bank's SWIFT electronic messaging system and were able to walk away with $81 million before systems in New York flagged the transfers.[50] Like innumerable hacks involving credit card fraud and identity theft, this attack was an instance of cyber theft motivated by an intent to steal money, not harm the security capabilities of Bangladesh.

Yahoo breach: In the fall 2016, Yahoo Inc. disclosed that in separate attacks during 2013 and 2014, as many as 1.5 billion user accounts were compromised. The attackers stole user information, passwords, and answers to security questions.[51] While the hackers did not acquire credit card information, answers to security questions would make it easier for hackers to gain access to users' accounts on other sites that might contain banking or credit card information. Law enforcement officials said the 2014 breach was probably the work of Russian hackers.[52] Yahoo claimed that a state-sponsored actor was responsible, but this has not been independently verified.[53]

Cyber Espionage

OPM hack: In April 2015, the Office of Personnel Management detected that its systems had been breached and that hackers had been siphoning data for at least one year. The U.S. government attributed the hack to China and reported that more than 20 million records with background checks and personal information were stolen.[54] Former and current intelligence officials have called the operation cyber espionage and have cautioned against calling for retaliation because the United States engages in similar activities.[55]

Russian hacks of the USG: In spring 2015, news reports revealed that Russian hackers had compromised the unclassified email systems of the State Department and White House.[56] While the hackers did not gain access to classified information, they were able to access sensitive data, including the president's non-public schedule and emails to and from the president. At the time, the State Department breach was considered the "worst ever" cyber intrusion of a federal agency.[57] It appears that espionage was the motivation.

[50] Krishna N. Das and Jonathan Spicer, "How the New York Fed fumbled over the Bangladesh Bank cyber-heist," *Reuters*, July 21, 2016. (http://www.reuters.com/investigates/special-report/cyber-heist-federal/); Syed Zain Al-Mahmood, "Bangladesh Central Bank Found $100 Million Missing After a Weekend Break," *The Wall Street Journal*, March 10, 2016. (http://www.wsj.com/articles/bangladesh-central-bank-found-100-million-missing-after-a-weekend-break-1457653764)

[51] Vindu Goel and Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," *The New York Times*, December 14, 2016. (https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html)

[52] Craig Timberg and Hayley Tsukayama, "Yahoo says 1 billion user accounts were hacked," *The Washington Post*, December 14, 2016. (https://www.washingtonpost.com/business/economy/yahoo-says-1-billion-user-accounts-hacked/2016/12/14/a301a7d8-b986-4281-9b13-1561231417c0_story.html?utm_term=.a81b20bad786)

[53] Alyssa Newcomb, "Yahoo Says 'State-Sponsored Actor' Hacked 500M Accounts," *NBC News*, September 22, 2016. (http://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-massive-n652586)

[54] David E. Sanger, "U.S. Decides to Retaliate Against China's Hacking." *The New York Times*, July 31, 2015. (https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html); Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016. (https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/)

[55] Damian Paletta, "U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach," *The Wall Street Journal*, June 25, 2015. (http://www.wsj.com/articles/SB10007111583511843695404581069863170899504)

[56] Evan Perez and Shimon Prokupecz, "How the U.S. thinks Russians hacked the White House," *CNN*, April 8, 2015. (http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/); Michael S. Schmidt and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *The New York Times*, April 25, 2015. (https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html)

[57] Evan Perez and Shimon Prokupecz, "Sources: State Dept. hack the 'worst ever,'" *CNN*, March 10, 2015. (http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html)

Chinese systems compromise U.S. military supply chain: In September 2016, the Pentagon's Joint Staff intelligence directorate issued an internal report warning that Chinese-produced Lenovo computers and devices might pose cyber espionage risks. The report claimed that the products might compromise Defense Department supply chains. Other Lenovo products were found to communicate information covertly back to Chinese intelligence agencies.[58] How China intended to use information gathered through these devices is unclear but it appears unlikely that this cyber espionage is an example of cyber-enabled economic warfare since it was not intended to affect the economic underpinning of the defense sector but rather directly harm military supplies.

Cyber-Enabled Information War

Russia promotes fake story to incite Germans against immigrants: In early 2016, a young Russian girl went missing in Germany for 30 hours. When she returned to her family, she alleged that she had been kidnapped and raped by a group of Middle Eastern immigrants. Investigators quickly revealed flaws in her story, and she recanted, but Moscow charged that the German government covered up the crime, and its news outlets promoted the false story. The allegations circulated widely on Russian-language outlets, especially within the Russian community in Germany who protested the government's willingness to accept Syrian and other Middle Eastern refugees.[59] The purpose of Russia's campaign appears to have been to undermine the government of Chancellor Angela Merkel. German intelligence chief Hans-Georg Maassen has since claimed that Russia tried to "manipulate public opinion."[60] The information warfare was cyber-enabled because Russia used social media and internet news to drive the story.

Russian election interference: During the 2016 election, elements of the Russian intelligence and security services conducted spear phishing and malware attacks against U.S. political parties and presidential campaigns. In October, the U.S. intelligence community and Department of Homeland Security publicly accused Russia of conducting these cyber attacks.[61] In December, the administration announced a series of measures aimed at punishing those responsible.[62] The intelligence agencies generally agree that Russia's goal was to undermine confidence in U.S. democracy[63] and "help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him." In January, the intelligence community released an unclassified

[58] Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," *Washington Free Beacon*, October 24, 2016. (http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/)

[59] Tim Hume and Carolin Schmid, "Russia cries cover-up in alleged migrant rape of 13-year-old in Germany," *CNN*, January 27, 2016. (http://www.cnn.com/2016/01/27/europe/russia-germany-berlin-rape/); Adam Taylor, "An alleged rape sparked tensions between Russia and Germany. Now police say it was fabricated.," *The Washington Post*, January 29, 2016. (https://www.washingtonpost.com/news/worldviews/wp/2016/01/29/an-alleged-rape-sparked-tensions-between-russia-and-germany-now-police-say-it-was-fabricated/?utm_term=.34934a9d299d)

[60] Andreas Rinke and Andrea Shalal, "Germany alarmed about potential Russian interference in election: spy chief," *Reuters*, November 16, 2016. (http://www.reuters.com/article/us-germany-election-russia-idUSKBN13B14O)

[61] U.S. Department of Homeland Security, "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," October 7, 2016. (https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national)

[62] Department of Homeland Security and Federal Bureau of Investigation, "GRIZZLY STEPPE – Russian Malicious Cyber Activity," *Joint Analysis Report*, December 29, 2016. (https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf)

[63] Adam Entous and Ellen Nakashima, "FBI in agreement with CIA that Russia aimed to help Trump win White House," *The Washington Post*, December 16, 2016. (https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html?utm_term=.0e440bfd69b2)

report on the interference concluding, "Russian President Vladimir Putin ordered the influence operation."[64] The operation was a classic case of cyber-enabled information warfare. Governments in Western Europe have expressed heightened concern that Moscow may try to repeat these activities during their upcoming elections.

Cyber Sabotage

Stuxnet virus: Beginning in 2008, a complex virus now known as Stuxnet infiltrated the control systems at an Iranian nuclear facility in Natanz. The virus, operating covertly for two years, altered the rotation speed of nuclear centrifuges, causing them to malfunction and self-destruct.[65] Although never publicly confirmed by Washington, the virus is believed to have been created by the United States and Israel, possibly in cooperation with other nations. The attack's intention was not to affect the Iranian economy – although it coincided with efforts to enhance unilateral and multilateral sanctions against Tehran – but rather directly to degrade Iran's military capabilities, in this case its military-nuclear capabilities. It may be premature to classify the Stuxnet effort as cyber warfare. However, as the terms of reference of cyber war and its components evolve, historians may determine that the Stuxnet campaign reflected one of the most successful examples of this new type of warfare.

Cyber Terrorism

Iran's attack against the Sands Casino: In February 2014, Iranian government hackers conducted a massive attack against the Las Vegas Sands Corporation, causing $40 million in damage and destroying as much as three-quarters of the company's computer servers.[66] The cyber attack was reportedly a retaliation for comments CEO and majority owner Sheldon Adelson made about bombing Iran over its illicit nuclear program. The hackers had no intention of damaging the broader U.S. economy or national security, but rather wanted to cause damage to a single company and thereby send a message to its adversaries. This attack was an act of cyber terrorism because it caused severe disruption and harm, was pursued as retaliation, and was intended to create fear among those who might speak aggressively against Iran or attempt to thwart its nuclear ambitions.

North Korea's attack on Sony Pictures: In late 2014, hackers, under orders from the North Korean government, infiltrated Sony Pictures' network, stealing, deleting, and later publishing large amounts of company data.[67] The attackers threatened terrorist attacks if the company released "The Interview," a comedic film about an assassination plot against the North Korean leader. The threat apparently succeeded as the studio pulled the movie from large theaters – although it later released copies for digital streaming, and the movie received a limited theatrical release in the United States and a broader release overseas. The attack appeared to have had limited, if any, effect on U.S. policy or on the U.S. economy, and seems to have been a cyber terrorist attack on an individual company, with an

[64] Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017. (https://www.dni.gov/files/documents/ICA_2017_01.pdf)

[65] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012. (http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html); Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014. (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)

[66] Jose Pagliery, "Iran hacked an American casino, U.S. says," *CNN*, February 27, 2015. (http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/); Benjamin Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, December 12, 2014. (https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas)

[67] Peter Elkind, "Inside the Hack of the Century," *Fortune*, June 25, 2015. (http://fortune.com/sony-hack-part-1/); David E. Sanger and Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," *The New York Times*, December 17, 2014. (https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html)

implied threat to others who might voice similar criticism of North Korea's head of state. In the aftermath of this attack, the U.S. publicly stated that the state-sponsored attack was a "violation of U.S. sovereignty 'coupled with an attempt to interfere with freedom of expression.'"[68] On January 2, 2015, the U.S. Treasury Department released a statement sanctioning three North Korean entities and ten individuals involved in the attack.[69]

III. Possible CEEW Attacks, More Information Needed

Russian sabotage of the BTC pipeline: In August 2008, hackers sabotaged the Baku-Tbilisi-Ceyhan pipeline, causing physical damage and lost revenues estimated at more than one billion dollars.[70] While at the time Turkey blamed Kurdish separatists for the attack, U.S. intelligence officials now believe it was perpetrated by Russia.[71] Russia long opposed the creation of the BTC pipeline and other efforts to bring Caspian and other oil and gas to the market bypassing Russia; however, it is unclear what Russia's motives were for sabotaging the pipeline. It is possible that the attack was intended as terrorism rather than economic warfare. The question is further complicated by the fact that three days later, the Russia-Georgia War began.

Iranian attacks against U.S. banks: Beginning in 2011 and continuing through 2013, Iranian hackers linked to the Islamic Revolutionary Guard Corps (IRGC) conducted numerous distributed denial of service attacks against at least 46 U.S. banks and financial services companies, including JP Morgan, Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, Fidelity, Capital One, American Express, and BB&T.[72] The U.S. Department of Justice indicted the Iranians responsible for these cyber attacks as well as the hacker responsible for separately penetrating the control system of the Bowman Dam in Rye, New York.[73] Iran's intention behind these attacks is unclear. Was Iran simply retaliating for economic sanctions and/or the recently discovered Stuxnet cyber attacks on its nuclear weapons program? Or did the Iranian government hope that by harming U.S. financial institutions, it could threaten the U.S. economy and convince lawmakers to change U.S. policies towards Iran? Greater information and analysis is necessary to determine if these attacks were part of a cyber-enabled economic warfare campaign or intended for other purposes.

Cyber sabotage attacks on Iran's energy sector: Iran's Oil Ministry and its affiliates were targeted in early 2012 in a series of cyber sabotage attacks, including attempts to destroy hard drives and data by insemination of the "wiper" computer virus.[74] Mohammad Reza Sabzalipour, president of the Tehran World Trade Center, argued that the purpose of the attacks was to "increase pressure so that Iran will compromise in the upcoming nuclear talks…

[68] Ellen Nakashima, "Why the Sony hack drew an unprecedented U.S. response against North Korea," *The Washington Post,* January 15, 2015. (https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?utm_term=.f5981a9b3bd5)

[69] The U.S. Department of the Treasury, Press Release, "Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea," January 2, 2015. (https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx)

[70] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg*, December 10, 2014. (https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar)

[71] Ibid.

[72] Dustin Volz and Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," *Reuters*, March 25, 2016. (http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF)

[73] U.S. Department of Justice, Southern District of New York, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities," March 24, 2016. (https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated)

[74] Saeed Kamali Dehghan, "Iranian oil ministry hit by cyber-attack," *The Guardian* (UK), April 23, 2012. (https://www.theguardian.com/world/2012/apr/23/iranian-oil-ministry-cyber-attack)

We are in a bloodless war. If the talks fail, Iran can expect much more of this," he said.[75] Nonetheless, more needs to be discovered about the identity and motivation of the attacker before these attacks can be determined to be an example of CEEW.

Russian "back doors": In addition to cyber crime for financial gain perpetrated by criminals,[76] Russia's operations in cyber space are characterized by deep penetration into public and private sector systems to explore, map systems, and establish future access points.[77] For example, former executives alleged in a suit against a company supplying fingerprint technology to the Pentagon that Russia may have installed back doors into the company's system.[78] As with most instances of Russian penetration into government and private systems, further investigation is needed to determine Russia's plans and intentions, as well as what linkages exist between specific incidents and Russia's long-standing support of the cyber crime networks that operate there.[79]

CyberBerkut hacks Polish websites: Pro-Russia Ukrainian hackers known as CyberBerkut attacked nearly 40 Polish government websites and the Warsaw Stock Exchange in August 2014, reportedly in retaliation for Poland's involvement in NATO and support for the Ukrainian government. The hackers took down the websites and replaced them with graphic images of the Holocaust.[80] Reportedly, the hackers stole and published client login information from the Warsaw Stock Exchange, creating additional challenges and rattling the public's confidence in the Exchange.[81] However, it is unclear if the hackers specifically targeted the stock exchange to cause economic damage, if the purpose was to influence government policies through cyber terrorism, or if the website was merely one of many targets of opportunity.

Chinese theft of Australian data: Since late 2014, trade between China and Australia has skyrocketed. At the same time, however, Australian mining and natural resource firms, as well as law firms involved in mergers and acquisitions, have experienced an unprecedented level of cyber attacks and intrusions.[82] The incidents appear to follow the same pattern of cyber espionage and intellectual property theft that China has conducted against U.S. companies, indicating that these incidents are likely part of a cyber-enabled economic warfare campaign against Australia, but additional study of the context and strategic intentions is necessary to make a conclusive judgment.

[75] Thomas Erdbrink "Facing Cyberattacks, Iranian Officials Disconnect Some Oil Terminals From Internet," *The New York Times*, April 23, 2012. (http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html)

[76] Jack Marshall, "Russian Hackers Stole Millions From Video Advertisers, Ad Fraud Company Says," *The Wall Street Journal*, December 21, 2016. (http://www.wsj.com/articles/russian-hackers-stole-millions-from-video-advertisers-ad-fraud-company-says-1482272717); "Russians Busted on Hacking Charges," *ABC News*, April 24, 2016. (http://abcnews.go.com/Technology/story?id=98625&page=1); Ilya Khrennikov, "New Russian Hacker Cell Hit 13 Banks Since August, Group-IB Says," *Bloomberg*, March 17, 2016. (https://www.bloomberg.com/news/articles/2016-03-17/new-russian-hacker-cell-hit-13-banks-since-august-group-ib-says)

[77] Sam Jones, "Cyber warfare: Iran opens a new front," *The Financial Times* (UK), April 26, 2016. (https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3)

[78] Bob Egelko, "Suit warns of Russian 'back door' into U.S. fingerprint systems," *SFGate*, August 14, 2016. (http://www.sfgate.com/nation/article/Suit-warns-of-Russian-back-door-into-U-S-9140446.php)

[79] Brian Whidmore, "Organized crime is Now a major element of Russia statecraft," *Business Insider*, October 27, 2015. (http://www.businessinsider.com/organized-crime-is-now-a-major-element-of-russia-statecraft-2015-10)

[80] Zach Wener-Fligner, "Pro-Russia Ukrainian hackers just replaced Polish sites with images from a Holocaust slaughter," *Quartz*, August 14, 2014. (https://qz.com/249860/pro-russia-ukrainian-hackers-cyberberkut-just-replaced-37-polish-sites-with-images-from-a-holocaust-slaughter/); "Ukrainian hackers claim attack on Polish websites," *Agence France-Presse*, August 14, 2014. (https://www.yahoo.com/news/ukrainian-hackers-claim-attack-polish-websites-193806386.html?ref=gs)

[81] Michael Riley and Jordan Robertson, "Cyberspace Becomes Second Front in Russia's Clash With NATO," *Bloomberg*, October 14, 2015. (https://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato)

[82] "Double-Edged Sword: Australia Economic Partnerships Under Attack From China," *FireEye*, October 13, 2014. (https://www.fireeye.com/blog/threat-research/2014/10/double-edged-sword-australia.html)

Possible Russian infrastructure sabotage: In December 2015, Russia allegedly orchestrated a cyber attack on Ukraine's electric grid causing widespread temporary blackouts.[83] However, further investigation is needed to determine whether the Kremlin authorized the attacks and, if so, whether it principally intended to cause serious economic harm or if this attack would be better characterized as cyber terrorism.

Cyber sabotage against Venezuelan banks: In December 2016, Venezuelan President Nicolas Maduro accused rightwing forces of attempting to "destabilise his government through financial 'cyber sabotage.'" Payment terminals and electronic banking platforms throughout the country went down, leading to a spike in the black market value of the dollar. In the wake of large public protests from citizens unable to make Christmas purchases, Maduro denounced the "economic, monetary coup d'état, by international financial sectors and some national financial sectors."[84] Intelligence services arrested the leadership of a financial transaction company for alleged involvement and openly accused members of the opposition party.[85] It is unclear, however, if the allegation are based on evidence or part of the authoritarian government's attempt blame others for the ongoing, massive economic crisis.

Conclusion

The language to describe cyber attacks has not kept up with technological innovations. State and non-state actors alike are engaging in malicious cyber activities, but Washington, its allies, and the private sector lack a common language to describe the battle in cyber space. As a result, cooperation between the public and private sector, as well as between and amongst governments and government agencies, is hampered. The U.S. government should work with its allies and the private sector to create a unified understanding of the key concepts broadly related to cyber attacks and, more specifically, related to cyber-enabled economic warfare. Understanding not only the terminology but also the tactics, strategies, and intentions of nation states, non-state actors, and criminal organizations is critical for crafting effective counter-measures and proactive policies.

[83] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016. (https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/); Jose Pagliery, "Scary questions in Ukraine energy grid hack," *CNN*, January 18, 2016. (http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/)

[84] Rachel Boothroyd-Rojas, "Venezuelan President Reports 'Cyber Sabotage' against Banking System," *Venezuelanalysis.com*, December 2, 2016. (https://venezuelanalysis.com/news/12819)

[85] Rachel Boothroyd-Rojas, "Venezuelan Intelligence Services Arrest Credicard Directors," *Venezuelanalysis.com*, December 5, 2016. (https://venezuelanalysis.com/news/12820)

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu