Cyber Enhanced Sanction Strategies: Do Options Exist?

Mark Peters*

ABSTRACT

Today's financial sanction practices need immediate updates to generate sufficient impact in modern crisis resolution and should consider cyber-based strategies. Globally, some erected, economic sanctions have existed for decades without achieving, or making significant progress towards, their desired effects. Cyber means could enhance sanction strategies to more effectively achieve national ends. The strategy suggested here designates a potential methodology as Cyber Enhanced Sanctions (CES) and advocates digital techniques to more effectively influence national decision-makers while allowing reversibility, secured communications, and humanitarian relief through digital channels. Examining current cyber means establishes a baseline for strategists to develop implementation strategies. Once a baseline strategy is proposed, this article further suggests a potential application case in U.S. sanctions against Russia concerning the Ukrainian conflict. Overall, CES could offer expanded options for the U.S. national power toolkit.

* *Lt. Col. Mark Peters* is the Operations Division Chief for the 625th Operations Center at JBSA-Lackland, Tex. Previously, he served as the Commander, 18th Intelligence Squadron, Wright-Patterson AFB, OH. He holds a Doctorate Degree in Strategic Security from Henley-Putnam University and has a forthcoming text from Potomac Books researching how states use cyber means to achieve economic ends.

JOURNAL OF LAW AND CYBER WARFARE

Volume 6 | Summer 2017 | Issue 1

INTRODUCTION

In 2014, Russia first invaded Crimea, promising help and solidarity to oppressed ethnic minorities. Ukraine followed on Putin's hit list with a separate invasion when the nation failed to fall in line with Russia's desired European Union trade guidelines. The United States and EU responded quickly with news conferences, stern démarches, and eventually, governmental actions generating economic sanctions. Current financial sanction practices sometimes fail to achieve desired timelines, missing targeted bank accounts or actors, and failing to create the desired response and influence decision makers. A cyber-based strategy may offer improvements to purely diplomatic financial sanctions in achieving national ends.

Sanctions, supported by national diplomatic and economic influences, are a traditional state answer to foreign crises with the most recent change being the use of targeted actions against individual actors. Some sanctions, such as those levied against Iran, required years before any actions were realized, implemented, and resolved, and even longer before any results could possibly be tracked to those effects.[1] Even if imposed sanctions start effectively, their actions may fail to impact intended targets. During recent U.S. sanctions against Russia relating to the Ukrainian crisis, several Russian leaders including Vladislav Surkov, a Putin advisor,

[1] In Iran's case, since 1979, eleven separate legislative acts describing economic sanctions and seventeen different Executive Orders have been applied to Iran to attempt to curb their behavior regarding Weapons of Mass Destruction proliferation and terrorist support. Dianne E. Remmack, *Iran: U.S. Economic Sanctions and the Authority to Lift Restrictions*, Congressional Research Service (15 Jul 2016) R43311.

and Dmitri Rogozin, a deputy prime minister, joked with national media about the United States' ineffectiveness in enforcing sanctions.[2] If traditional sanctions falter, the choices available to senior leaders rapidly narrow and may lead to deciding between costly, military action and perceived national ineffectiveness. Cyber means offer an approach to augment U.S. economic sanction effectiveness without a boots on the ground commitment.

Current financial sanction strategies delay national ends through time-consuming methods and frequently fail to significantly change the sanctioned state's decision calculus. The lack of effective alternatives, unreachable targets due to conventional economic structures, and minimized communication channels to those harbored by hostile governments, can prevent sanctions from reaching their full potential in a timely manner. Cyber technology offers some alternatives through combining cyber means with economic sanction employment to target selected financial targets. Strategies emphasizing cyberspace tools may enhance economic sanctions and improve effectiveness through: increased enforcement opportunities, targeted economic denial and disruption, immediate reversibility upon success through ceasing cyber effects, increasing communication channels to threatened populations, and finding alternatives for improved humanitarian relief. Herein, a Cyber Enhanced Sanction (CES) is defined as employing active cyber techniques to support state-established economic sanctions guidelines. CES cyber techniques would seek to target vulnerabilities in digital financial transactions to delay or disrupt their execution, while coordinating with political decision-makers to achieve sanction goals.

---

[2] Stephen Lee Mylers & Peter Baker, *Putin Recognizes Crimea Secession, Defying the West,* N.Y. TIMES, March 18, 2014.

The CES strategy exploration builds through four areas. The first two are theoretical; examining current sanction practice shortfalls, and then discussing strategies underlying sanction enhancement through cyber. The next two areas focus on proposed CES means: examining publicly available CES techniques and limitations, and next evaluating a proposed CES framework, which could have been employed during the current Ukrainian conflict by the U.S. against Russia. Modifying publicly available cyber techniques would support the proposed effect categories and increase influence on sanction outcomes from a foreign leader's decision calculus, to increasing public unrest, or even cause a head of states outright removal. The modifications suggested are theoretical in this paper, strategies are outlined, but individual techniques would have to be developed for each sanction event. Cyber means still face limitations including escalation fears, legal constraints, and technical challenges in access and tool availability. Each limitation creates potential challenges for both policy and operational implementation even if they are successfully mitigated. After weighing the generic options, one can move to consider currently published U.S. guidance and standards as they could apply to cyber technique applications in the Ukrainian crisis and potential effectiveness metrics.

I. WHAT'S WRONG WITH CURRENT SANCTION PRACTICES?

Sanctions employ national power means, usually economic, to create effects. Current practices simply take too long to work but evaluating current practices first requires obtaining common definitions. In policy, power is, "the ability to affect other people to get the outcomes one

wants."[3] Sanctions are the, "deliberate, government-inspired withdrawal, or threat of withdrawal, of customary trade or financial relations."[4] An economic sanction definition specifies, "[o]rganized actions governments take to change the external environment in general or the policies and actions of other states in particular to achieve the objectives . . . set by policy makers."[5] All three explanations drive discussion on sanction ways and ends without considering means. The term cyber means suggests using a cyber-based technique to link overall objectives to lower level effects. For example, preventing a bank from issuing funds to purchase nuclear fuel by denying access to servers containing financial accounts. Multiple commonly accepted cyberspace definitions appear within academic and operational literature. One of the broadest refers to cyberspace as a "man-made environment for the creation, transmittal, and use of information in a variety of formats."[6] A more technical definition cites cyberspace as, "an agglomeration of individual computing devices that are networked to one another . . . and the outside world."[7] Nye cites cyber power as, "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[8] In the national power spectrum, cyber uses microforce compared

---

[3] JOSEPH S. NYE, CYBER POWER at 2 (2010).
[4] Yitan Li, *US Economic Sanctions Against China: A Cultural Explanation of Sanction Effectiveness, in* 38-2 ASIAN PERSP. 311, 312 (2014).
[5] *Id.*
[6] GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE (2001).
[7] MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 6 (2009).
[8] JOSEPH S. NYE, CYBER POWER 4 (Belfer Ctr. for Sci. & Int'l Affairs, Harvard Kennedy School 2010).

to the megaforce reserved for nuclear weapons.[9] CES offers these microforce means as an enhancement after an initial sanctioning decision to help create timely change.

Microforce theory emerged from Gregory Rattray's information warfare discussions. In addressing interstate cyberpower strategically, Gregory Rattray used cyber as his primary action showing how states achieve ends with information. He delineates cyberpower as when, "state and nonstate actors [use cyber means] to achieve objectives through digital attacks on an adversary's centers of gravity"[10] He avoids using cyberspace regularly, preferring its interpretation as a domain rather than a separate construct. Rattray also avoids discussing economic centers of gravity as information vulnerabilities. His theory's military cyberpower concentration likely explains why he ignores addressing diplomatic and economic vulnerabilities.

One of Rattray's main contributions to cyber applications occurs in categorization. He establishes the term "microforce" for digital attacks as a function other than a conventional kinetic weapon, or the nuclear megaforce examined in deterrence discussions.[11] Later discussion here links these terms with qualitative categories for evaluation. Rattray frames information warfare requirements as complex interconnections, civilian technological leadership, a fast change rate, and global interconnection between operations and production. As important, he details what conflict characteristics define where a state could seek cyberpower advantages, such as when an offensive advantage exists, a significant vulnerability is present,

[9] RATTRAY, STRATEGIC WARFARE IN CYBER SPACE 20 (2001).
[10] *Id.* at 14.
[11] *Id.* at 12.

minimal opportunity exists for retaliation, and effects are observable.[12]

Understanding the basic definitions above allows returning to why sanctions sometimes fall short in application. Economic sanctions present the primary means for international organizations like the United Nations (UN) to manage crisis. In the late 1990's, practices shifted from broad economic sanctions denying all financial activity to specific commodities, and then to targeting individuals. Individuals do not always appear relevant to national policy impacts although post-crisis link analysis frequently uncovers connections. CES theory suggests exposing sanctioned individuals through cyber techniques, as previously highlighted by established UN practices, may influence their decision-making and create desired government changes without collateral population impacts.[13] CES goes beyond merely naming individuals in diplomatic documents to influence multiple economic vulnerabilities across the global cyber commons.

Economic sanctions historically work based on the intended receiver's threat perception. Ang and Peksen's study traced sanction effectiveness to asymmetric perceptions, issue salience and outcome.[14] These elements tie foreign policy makers' perceptions on international conflicts, whether issues are personally relevant, and how domestic policies drive international outcomes. The applied

---

[12] *Id.*

[13] Peter Wallensteen & Helena Grusell, *Targeting the Right Targets? The UN Use of Individual Sanctions*, *in* 18-2 GLOBAL GOVERNANCE 208-09 (2012).

[14] Adrian U-Jin Ang & Dursun Peksen, *When Do Economic Sanctions Work? Asymmetric Perceptions, Issue Salience, and Outcomes*, 60 POL. SANCTIONS Q. 142 (2007).

Russian sanctions did not pose either a national or personal threat to Russian leaders. CES options help shift from broad-based applications to the financial influences linked to Russian oligarchs through identifying and selecting digital options tied to the individual. Disconnects between the Russian people and their leaders' exploitations have emerged over recent crises, and CES options could help expand those gaps.[15] Modern attempts to sanction Iran demonstrated where financial sanctions proved to be neither timely nor effective.[16]

A. Sanction Theories

In a broad-based discussion, theoretical applications provide a knowledge base while specific strategies and techniques appear in the next section. Sanctions are sometimes considered a blockade option in denying or disrupting trade.[17] World War I associated efforts used blockades to deny entire ports or prevent trade goods from shipment. As a denial and disruption means, financial sanctions serve three general purposes: denying individual

---

[15] FIONA HILL & CLIFFORD G. GRADDY, MR. PUTIN: OPERATIVE IN THE KREMLIN (2013).

[16] This Congressional report provides a detailed review of all sanctions associated with Iran and a quick look at their effectiveness. Obviously, Iranian sanctions have not succeeded as expected but a full effectiveness discussion is beyond the scope of this paper. KENNETH KATZMAN, RS20871, IRAN SANCTIONS (2017).

[17] The US Navy defines blockade as, "a belligerent operation to prevent vessels and/or aircraft of all nations, enemy as well as neutral, from enter or exiting specified ports, airfields, or coastal areas belonging to, occupied by, or under the control of the enemy nation." U.S. NAVY, MARINE CORPS & COAST GUARD, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, Ch. 7.7, (Dep't of the Navy 1995).

finances, disrupting government functions, and ensuring humanitarian relief.[18] Rabkin and Rabkin show a clear comparison exists between cyber means and blockade usage in influencing economic outcomes without physical harm.[19] This CES theory attempts to expand national options through access, breach, disruption and denial techniques. Traditional sanctions can manipulate economic impacts by changing names and accounts on documents before global distribution to banks and merchants. Most sanctions only create effects in implementing countries, for example, preventing Russian oligarchs from reaching their U.S. bank accounts. Altering digital code could create global pressure through influencing selected individuals in their home countries while white-list techniques allow humanitarian relief to pass through enacted controls.[20]

Wallensteen suggests targeted sanction employment improves through gradually escalating pressure.[21] Gradual escalation only applies if the desired pressure influences decision-making calculus manageably. For instance, it is difficult to control cooking temperatures with a blowtorch, but easier with an electric oven. Escalation is critical in scaling effects to desired results. Managing sanction pressure requires being able to increase a tool's breadth, such as an imposed sanction denying several Russian leaders their

---

[18] Joy Gordon, *Smart Sanctions Revisited*, *in* 25-3 ETHICS & INT'L AFF. 315, 327 (2011).

[19] Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the War at Sea*, 14 CHI. J. INT'L L. 197, 215 (2013).

[20] White lists describe actions where particular named activities are allowed to pass through a digital or physical barricade. Only the activity identified on the white list designations can cross the barriers. All other actions are diverted away or denied by the enforcing agent, whether digital or physical security.

[21] Wallensteen & Grusell, *supra* note 15, at 216.

U.S. bank account access that could be enhanced by adding additional leaders or restricting access to more commercial and financial institutions. CES options would move past denying only U.S. bank account activity to deny additional transactions to sanctioned entities in their own state. Rapidly changing a selected individual from government approved sanction lists in an implemented cyber technique allows CES options to increase sanction efficiencies. CES enforcement would not require multiple rounds of diplomacy and coordination, only implanting the tools within the desired financial networks. Global CES applications complement interdependence theory and also support realist and liberal international relations approaches.[22]

Targeted sanctions seek three basic outcomes: to bring leaders to the bargaining table, deprive resources to create regional power shifts, and threatening increased sanctions.[23] Cyber enhancement impacts all outcomes through increased sanction possibilities. Network means potentially deny individual's access to not just local resources, but to any digitally accessed finances worldwide. Although their legality may be questionable in any one state, actions could be authorized under broader multinational options such as the U.N. Security Council or NATO. Digitally manipulating accounts allows one to shift resources from a sanctioned account to provide congressionally approved funding to local opposition groups. Sanctioning activities that occur through cyber could be done with or without the support of organizations in the

[22] ROBERT KEOHANE & JOSEPH NYE, POWER AND INTERDEPENDENCE 252 (2012). ALISON LAWLOR RUSSELL, CYBER BLOCKADES 24-26 (2014).
[23] Wallensteen & Grusell, *supra* note 16, at 210.

offending state. Of course, offensive cyber actions against another state, even if justified by international agreements fall in a less defined area of international policy. U.S. Executive Orders (EO) sanctioning Russia over Ukrainian involvement only block properties within the United States' possession.[24] Cyber offers global power expansion within sanction planning, without committing local troops or the national resources required for traditional enforcement while increasing effectiveness. Cyber techniques can move past older means to disrupt or deny any digital system, worldwide.

CES techniques will demonstrably enhance sanction effectiveness. Historical sanction evaluation metrics measured whether sanctions affected target states' decision-making calculus.[25] CES effectiveness should also not be tool-centric, but evaluate sanction efficiency. For instance, with a Stuxnet-like example, effectiveness would not measure individual centrifuge operations but the overall effect on the Iranian nuclear development program. One study examining eight-targeted UN sanctions without cyber enhancements estimates sanctions achieving national goals at a 20-34% rate.[26] Sanctioned activities are frequently complex, and continuing data analysis will hopefully provide more comparative data. Wallensteen's study's biggest shortfall is the original data's age, at 20–30 years old, which coincides with the beginning of Iranian sanctions. Modern sanction effectiveness studies are rare, with most using qualitative case studies rather than quantitative

[24] Exec. Order No. 13660, *Blocking Property of Additional Persons Contributing to the Situation in Ukraine*, 79 Fed. Reg. 53, THE AMERICAN PRESIDENCY PROJECT (2014)
[25] Gordon, *supra* note 20, at 315-335.
[26] Wallensteen & Grusell, *supra* note 16, at 225.

assessments. Kozhanov, studying U.S. sanctions on Iran, highlights how policy loopholes can delay successful sanction employment.[27] Most loopholes consist of newly emerging activities or unreachable financial transactions. Cyber-enhancement would allow altering sanctions based on Treasury approved lists and close loopholes between financial means in one country and industrial production in another. CES means could highlight individuals, corporations, and products for explicit effects while traditional sanctions may persist for years without significant impacts. U.S. sanctions on Iran have generated only minimal behavior changes since their 1984 inception.[28] Modern resource constraints mean even small behavioral improvements in an adversary may be worthwhile investments in new means.

B. Sanction Legality

National power employment always depends on international perceptions. Effective sanction enhancement should enforce justice while remaining within national and international legal boundaries. CES should function with declared sanctions, through reaching other global cyber commons areas to disrupt and deny channels. Evaluating overall sanction legality is also left for other discussions. Some CES actions affecting foreign institutions may move from a typical sanction action to a cyber-attack, although short of physical harm. A starting point for CES legality

---

[27] Nikolay A. Kozhanov, *U.S. Economic Sanctions Against Iran: Undermined by External Factors*, *in* 18-3 MIDDLE EAST POLICY 144, 144-160 (2011).

[28] Jeffrey J. Schott, *Economic Sanctions Against Iran: Is the Third Decade the Charm?* Vol. 47 NAT'L ASS'N FOR BUS. ECON. (2012).

should be applicable international standards and UN due process considerations. Specific correlation to international law is essential to ethical cyber employment, and this will likely be the sanctioning power's responsibility during implementation.[29]

CES actions could be undertaken covertly. Many consider covert action statutes and regulations sufficient oversight for covert cyber actions. A post-1947 U.S. covert actions review refers to them as an option between overt military intervention and diplomacy.[30] American constitutional doctrine calls for power separation between legislative and executive branches when authorizing specific Presidential powers. Covert action requirements currently state that congressional committees should be informed with written findings prior to initiation.[31] CES implementation approvals outside the public purview would most likely occur here. Covert actions fall outside typical Title 10 (Military) and Title 50 (Intelligence) authorities, although internal oversight does exist.[32] Working within these guidelines could create oversight for digital actions generating physical effects.

CES employment will likely follow an implementing power's initial sanction declaration and delivery. LOAC questions emerge as some cyber tools are currently

---

[29] Although unethical tool use has been a human possibility since first picking up a stone, one hopes that individuals and nations prefer legal and ethical approaches.

[30] L.K. Johnson, *Intelligence Analysis and Planning for Paramilitary Operations*, 5 J. NAT'L SEC. L. & POLICY 481 (2012).

[31] Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 MICH. L. REV. 423, 428 (2012).

[32] U.S. Government. "Armed Forces." Title 10, United States Code. Mar 1, 2012. U.S. Government "War and national defense." Title 50, United States Code. Mar 1, 2012.

positioned within military inventory and under acting commanders. While some scenarios may be considered cyber-attacks, CES does not advocate attacks on sovereign states, instead seeking to enhance existing unilateral or multilateral sanctions. The dividing line remains narrow, but sufficient enough to provide potential national power opportunities. When nations consider actions, which may be regarded as attacks, the Law of Armed Conflict (LOAC) should always be a primary reference. Academic writings have considered legality associated with cyber-attacks in some depth, so only a short overview is presented here.

Four areas are routinely considered as LOAC guidelines: proportionality, necessity, distinction, and chivalry. The best examination emerges from using concrete examples. During later discussion, the current U.S. EO 13660 series describing sanction employment against Russia in the current Ukrainian crisis provides relevant examples.[33] Proportionality prevents force use exceeding those necessary to attain military objectives; so here, cyber microforce should be the minimal force required to deny resources to declared individuals. Force must also be in proportion to the current conflict, for example, nuclear responses are not authorized for an attack involving automatic weapons. Theorized CES employment should not create overtly physically damaging effects, even if secondary or tertiary effects may occur. Necessity means utilizing minimal force to achieve objectives. Executive guidance will help to determine specific objectives. EO 13660 allows the Department of Treasury (DoT) and the Office of Foreign Asset Control (OFAC) to designate sanctioned individuals.[34] Distinction involves

[33] Exec. Order No. 13660, *supra* note 26.
[34] *Id.*

discriminating between combatants and non-combatants to engage with only valid targets. The Geneva and Hague conventions require all combatants to have a commander, fixed insignia, carry arms openly, and conduct operations in accordance with law.[35] Since most EO-identified, sanctioned individuals are non-military, and are not being attacked by physical force, distinction should be waived.[36] Finally, chivalry involves recognizing traditional emblems such as white flags and red crosses. Although they are not traditionally employed during cyber engagements; cyber tools could be constructed to allow humanitarian donations recognized by 50 U.S.C 1702(b)(2) and listed within EOs to avoid sanctioning, and in effect, create a digital Red Cross on network transactions.[37] Thus, any LOAC concerns regarding CES would appear to be initially satisfied.

Recent law of war changes treat cyber as an information weapon. No U.S. congressional limitations restrict cyber separately under LOAC, but a potential for perceived misuse emerges from civilian damages inflicted through indirect effects.[38] The Geneva Convention, Additional Protocol I (API), Article 58 requires military forces to attempt to remove civilian populations from affected areas and avoid locating military objectives near

---

[35] Ingrid Detter, THE LAW OF WAR at 136 (2000).

[36] Cyberattack is commonly defined as, "[a] cyber-attack consist[ing] of any action taken to undermine the function of a computer network for a political or national security purpose[s] . . . . [T]he best test of whether a cyberattack is properly considered cyber-warfare is whether the attack results in physical destruction, sometimes called a 'kinetic effect,' comparable to a conventional attack. Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 826, 841 (2012).

[37] Exec. Order No. 13660, *supra* note 26.

[38] Detter, *supra* note 37, at 273.

densely populated areas.[39] Both sections pose issues if CES strategies involve attacks, which incorrectly identify individuals. Ninety-eight percent of all government communications pass over civilian networks and increase separation difficulties for targeting cyber techniques.[40] Cyber will increase implementation speeds and may cause some selection errors, but also increases correction speeds. The United States is an API signatory, although this particular section still lacks senatorial advice and consent. Further, cyberspace restrictions may require reevaluation of CES strategies if they occur in conjunction with international operations. UN due process standards may be a more beneficial lens to derive future regulations.

UN due process methods include notification, an individual's right to be heard, and actions prior to enforcement.[41] Past UN reports show no existing process fully validates submissions, as any member state may submit nominations at any time. Current U.S. sanctions concerning Russia delivered public notification of their intent through the DoT's website.[42] The UN right to be heard prefers considering individual challenges prior to when nation's implement sanctions. Governments using CES will likely react to an emerging crisis, and individuals would present delisting claims to the UN only after formal sanctions are in place. Finally, no prior due process examples for CES cases exist. Methods could likely follow restricted notification

---

[39] Eric T. Jensen, *Cyberwarfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1549 (2010).
[40] *Id.* at 1533.
[41] Kuho Cha et al., *United Nations Security Council Sanctions and the Rule of Law: Ensuring Fairness in the Listing and De-listing Process of Individuals and Entities subject to Sanctions*, [13 No. 2] THE WHITEHEAD J. DIPLOMACY & INT'L REL., 133-52 (2012).
[42] Exec. Order No. 13660, *supra* note 26.

procedures similar to the US Foreign Intelligence Surveillance Act (FISA) court. Arguments suggest public activities, like Russia's Crimean annexation, self-select certain individuals for retaliation while some persons may remain unaware of their own roles in their nation's actions. Publicly identified individuals could, theoretically, judicially challenge enacted sanctions at any time from declaration through employment. The current U.S. EO 13660 series sanctioning Russia identifies, in section 7, a Presidential determination stating sanction effectiveness depends on no prior notices before initial publications.[43]

Current sanctions have problems, which cyber means could solve. Developing cyber definitions allows a common framework to coordinate activities. Sanctions have been used before in international relations and years of examples demonstrate how and when certain techniques may be applied. Most importantly, studies illustrate where sanctions have success. Reviewing legality and process constraints illustrates where current sanctions are limited in application and a broader CES strategy involving cyber-attacks creates opportunity for policy makers. Using CES strategies to mitigate current sanctions shortfalls requires explaining the interdependence lens underlying cyber means.

II. WHAT STRATEGIES SUPPORT CYBER MEANS?

Interdependence theories state military power's importance decreases as international communication increases, but military cyber means allow for continued influences. Traditional Clausewitzian strategy envisions war as the extension of politics by other means, while modern theorists propose hard, soft, and smart national power

[43] *Id.*

applications. Many nations already employ a mixed power palette to influence international opinions. Cyber must become another brush within the U.S. national toolkit to paint the desired picture for tomorrow's world. The single brush used for traditional sanctions is insufficient, although CES offers a variety of brush sizes.

Cyberspace revolves on information manipulation. Static and dynamic information changes can drastically alter functionality and user impacts. Original functionality studies are too narrow to appreciate cyber usages, as global interdependence trends increasingly gain velocity through new developments. One can see globalism trends in economic, military, environmental and cultural tendencies. These trends are not uniform practices and vary by operational canvasses across the world. Cyberspace elements link functionally through interconnected information, to allow unique channels between individuals. Increased institutional velocities across networks adjusts not only message speeds, but how quickly an organization's structure may change to adapt to incoming information. Complex interdependence theory, while historically focused on softer applications, like monetary policy, allows coercive cyber teeth within sanctioning strategies.[44]

In the past, theorists relied on older strategies to drive cyber implementation without grasping strategic impacts.[45] These shortfalls limited vision and failed to spur creative power employment. Developing cyber means to accentuate cyberpower applications remains theoretically

---

[44] ROBERT O. KEOHANE & JOSEPH S. NYE, JR. POWER AND INTERDEPENDENCE (4th ed. 2012).

[45] Joseph S. Nye & William A. Owen, *America's Information Edge*, FOREIGN AFFAIRS: BLOG (Mar./Apr. 1996), https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge.

similar to the advantage gained when air forces improved from ballistic bombs to GPS-guided weaponry. Cyber techniques offer the opportunity to target specific resources, deny access to terrorists and adversary nations, and control global economic channels. Creative approaches ensure policy makers leverage new techniques and domains effectively.

A standard national power toolbox contains Diplomatic, Information, Military, and Economic (DIME) options. Power can be employed creatively anywhere, although targeted trade and financial sanctions are a frequent choice. Targeted trade sanctions disrupt particular commodities, while financial sanctions may blacklist persons and companies, categories of individuals, or target states and wide groups.[46] Blacklists identify individuals with whom the sanctioning entity forbids contact through freezing foreign financial assets.[47] Cyber enhancement allows denying sanctioned individuals, organizations, or assets within non-U.S. locations. The policy maker's only challenge may be deciding whether to characterize cyber-enhanced financial disruption as a hard, soft, or smart power application.

Typically, power uses are divided between hard and soft applications. While power remains the ability to make one act, hard power entails coercive methods like military force, while soft power addresses attractive elements like persuasion. Soft power is often viewed as a kinder, gentler approach to achieve desired end-states. Any targeted

[46] Gordon, *supra* note 20, at 327.

[47] Blacklists describe where a full list of all prohibited individuals is maintained by the controlling entity. In most network security, a blacklist would comprise the IP addresses of known malicious actors or sites the security function did not wish users' visiting.

sanction not including kinetic military force could employ soft power.[48] Cyber enhancement allows military cyber experts to contribute fully to soft power employment. The information revolution creates the illusion all nations possess similar soft power. Soft power influences require transmission mediums and, despite cyber's low entry costs, entry barriers for produced visual media, such as movies, which remains high. If measuring international influence, U.S. targeted sanctions employing soft power in Iran, Egypt, and Syria have been relatively ineffective.[49] Some nations have integrated soft power to negate smaller countries' information gains, although U.S. public successes employing softer, cyber means appears limited.[50] Blending military cyber expertise to CES strategies may regain some international, U.S. advantages.

Channels existing in an interdependent world-view allow smart power means to create effects. Power theories describe behavioral effects as coercion or attraction, while smart power combines hard and soft techniques through contextual intelligence applications. Nye defines contextual intelligence as understanding both the strengths and shortfalls of national, and specifically U.S. power.[51] Smart power through sanctions first appeared in the late 1990's when the United Nation's shifted to targeting financial sanctions against individuals and organizations, rather than

---

[48] Christopher A. Ford, *Soft on "Soft Power"*, *in* 32-1 SAIS REVIEW 90 (2012).
[49] *Id.* at 95.
[50] Nye, *supra* note 10.
[51] Joseph S. Nye, *Get Smart: Combining Hard & Soft Power*, FOREIGN AFFAIRS: BLOG (July/Aug. 2009), https://www.foreignaffairs.com/articles/2009-07-01/get-smart.

entire nations to limit negative humanitarian impacts.[52] Smart power theory describes the U.S. military power as unipolar, because economic relations are multipolar, and transnational relationships as inherently chaotic. While interdependent aspects lend stability to transnational relationships, that stability will be limited physically and temporally. Utilizing contextual intelligence to describe selected power relationships within a narrow scope allows tool development to match desired outcomes.[53] CES strategies are perfectly placed to enhance smart power options.

Cyberspace techniques are as varied as their kinetic cousins with the two most common categories being attack and exploitation. Planning CES strategies requires understanding what constitutes exploitation, when it becomes an attack, and when continuing actions cross state redlines. Experienced cyber theorists still frequently debate where lines between the three definitions emerge. Means labeled as cyber-attack may be necessary to achieve CES objectives. Targeting individuals, just like UN methods, allows CES methods to remain below cyber-conflict standards and redlines while still accomplishing national objectives.

Cyber-exploitation differs from cyber-attack by not fully depriving users of the system value. Martin Libicki provides three exploitation factors; no consequential harm, difficult to detect, and not recognized as *casus belli* by law of war.[54] CES-associated actions may appear as exploitation or attack forms through impacts. Those actions which

---

[52] Wallensteen & Grusell, *supra* note 15, at 208.
[53] Nye & Owen. *supra* note 47.
[54] MARTIN C. LIBICKI CYBERDETERRANCE AND CYBERWAR, at 23 (2009).

become attack may create legal concerns; the strategy should follow similar approaches to drone conflicts, focusing on where a CES cyber-attack creates no physical harm, and prevents an imminent threat. When policy makers plan CES during various international crisis events, financial or resource denial effects without physical damage will likely be a preferred U.S. option. Some attacks will first require exploitation and all exploitation requires prior access. Cyber methods could include denial of service on institutional websites, accessing and changing individual account information, or using realigning previously state funds to support congressionally approved opposition activities either publicly or covertly. Categorizing techniques as attack or exploitation will likely be less relevant to planners than overall sanction effectiveness.

Cyber-attack, from the State Department legal advisor, Harold Koh in a September 2012, US Cyber Command conference, and cited in Rabkin and Rabkin, must cause, "death, injury, or significant destruction [which] would likely be viewed as a use of force".[55] Academic cyber-attack definitions are more loosely structured like Hathaway et al.'s cyber-attack definition as, "any action taken to undermine the functions of a computer network for a political or national security purpose"[56] CES strategies including attack means should center on depriving an individual or organization of an information asset's economic value. Cyber-attacks meeting Koh's definition are usually considered cyber-warfare and may trigger self-defense rights under the UN Charter's Article 51. However,

[55] Rabkin & Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the War at Sea*, [14 No. 1] CHI. J. OF INT'L L. 197 at 200 (2013).
[56] Hathaway, et. al. *The Law of Cyber-Attack*, [100 No. 4] Cal. L. Rev. 817, 826 (2012).

Hathaway et. al. also makes the same differentiation as Koh regarding physical destruction when discussing triggered self-defense rights. CES methods may be considered illegal by the sanctioned country but should not cross any redlines or invite retaliatory attack.

Policy makers remain unconvinced cyber solutions offer valid international alternatives. Libicki in, "Brandishing Cyberattack Capabilities" explains how once a capability emerges, nations will be credited with those capabilities, regardless of actual employment.[57] Cyber-tools will be credited both when adversary systems work correctly and when they fail. Crediting cyber means with attack regardless of employment techniques allows planning to use their full potential. Properly placed messaging could affect one's decision calculus through suggesting unaligned effects actually connect to CES. Messaging resource costs, especially through social media, could be relatively small. Comparatively, the U.S. Department of Homeland Security has spent millions, if not billions of dollars, preparing to defend Critical Infrastructure and Key Resources (CIKR) vulnerabilities from attack. For planners, cyberspace defenses will remain critical and network vulnerability assessments are central within those discussions.

In cyberspace operations, access is paramount. Vulnerability and threat are often paired elements. Conducting cyberspace operations requires developing both a tool and access vector. Multiple versions of both will be needed during any extended sanction efforts. Implementing actors will likely see cyber-sanctioned networks rapidly striving to fix vulnerabilities even if the network intrusions

[57] MARTIN C. LIBICKI, BRANDISHING CYBERATTACK CAPABILITIES, at 12 (2013).

are undetected.[58] Original sanctions tell a bank to deny certain actors their services, CES methods merely tell the network to deny services to digital customers. Closing vulnerabilities will harden the target and require additional resources committed to redesigning networked tools for continued use. Once a vulnerability is closed, new access may be required to reach the same effect. CES techniques will likely need constant development, alteration, and adjustment to reach desired effects.

III. WHAT EMPLOYMENT TECHNIQUES SUPPORT CES?

A key to CES employment is determining which tools generate desired effects. Cyber-enabled actions seek to deny network accesses from targeted actors through multiple means. Several well publicized cyber-attack and exploitation techniques are evaluated here for potential usefulness as a baseline model while the overall employment focus remains on the Ukrainian case. Discussed cyber techniques to complement sanction activities include breach, disruption, functional denial, and global denial. Political and technical limitations are also considered. These CES options provide primarily for targeted potential means in an international conflict. A theoretical Ukrainian CES employment plan, based on current U.S. policy, would identify government websites associated with targeted individuals, public-facing email, or corporate websites. U.S. targets for sanction appear within DoT lists, Executive Orders, and current law. Most nations and cyber-operators guard cyber-attack techniques zealously so using publicized attacks as potential CES foundations avoids wandering into unsupportable debates

[58] Martin C. Libicki, *Cyberspace Is Not a Warfighting Domain*, [8 No. 2] I/S: A J. OF L. AND POLICY FOR THE INFO. SOC'Y 331, (2012).

about how an option could be employed. CES means may vary greatly between nations depending on covert capabilities and accesses.

A. Technique

Modifying public techniques to create unique cyber effects enables wider CES planning without revealing access techniques or zero-days. The first suggested option, breach, evolves from the 2014 Target data breach and DigiNotar certificate theft. The second technique, disruption, examines the Qassam Cyber Fighters' multi-year DDoS against multiple U.S. banks and associated corporate websites. The third suggestion, functional denial, models Russian combined arms methods within the Georgian conflict as well as efforts demonstrated in Crimean and Ukrainian actions. Finally, global denial is largely theoretical and proposed eliminating all cyberspace access for the sanctioned target. Developed options suggest some initial options while leaving the far edges of possibility for later planning.

1. Breach

The first option, breach, exposes network vulnerabilities. Breach means strive to create persistent network access. Digitally identifying individual accounts through national or open-source intelligence utilizes CES strategies similar to the popular Target or DigiNotar data breaches. Breach generates increased access and knowledge regarding activities within crisis areas.

As an example, in 2013, Target, a large US retailer, experienced significant network breaches. This breach used third party vendors for initial accesses, positioned malware on Point of Sale (POS) devices, and removed consumer data

from compromised systems. The breach path obtained over 40 million user credit records and 70 million data files.[59] The two-stage attack succeeded due to careful attacker planning and poor Target security measures. Similar planning methods support CES strategies to demonstrate that sanctioned entities are inadequate in protecting constituencies. Protecting populations from outside threats is vital to both image and operations for most national governments. A government who cannot protect their population could likely lose face during international negotiations and local elections.

Breach means could target sanctioned corporations to generate data for other CES strategies. Russian corporations who experienced continuous disruption, functional denial, and breach would face marketability declines, creating additional government pressures to change policies. Applied pressure seeks CES's end goal through enhancing sanctions against national decision makers. The Target breach collected unencrypted data from POS infrastructure vulnerabilities and used syntactic malware to tag and exfiltrate information. Target's data was transferred to Russian criminals and sold on the black market.[60] This example highlighted organizational and individual impacts

[59] U.S. Senate Committee on Commerce, Science, and Transportation. *A "Kill Chain" Analysis of the 2013 Target Data Breach* (2014). From https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiO2JX50KfUAhWCSyYKHZeYBhUQFgglMAE&url=https%3A%2F%2Fwww.commerce.senate.gov%2Fpublic%2F_cache%2Ffiles%2F24d3c229-4f2f-405d-b8db-a3a67f183883%2F23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf&usg=AFQjCNFotjLB0rDJZO-j_46n5vWhxJ31wg

[60] Committee on Commerce. *A "Kill Chain" Analysis*, (2014).

available by compromising initial interactions and archival data. These methodologies support a CES strategy. Rather than apply a broad data vacuum, breach tools installed across POS systems could work to deny identified users from reaching their financial accounts. Once monetary accounts are identified, sanctioning agencies could transfer captured funds and account ownership to international aid organizations or selected opposition groups.[61] This transferal approach is similar to the current bill, S939, the "EL CHAPO Act", introduced in the U.S. Congress which proposed using seized property from a known criminal, in this case the Mexican drug kingpin, El Chapo, to fund border security measures.[62]

Individual breaches would highlight those areas sanctioned by U.S. or allied organizations. A single compromised account or system could prove sufficient to deny requisite financial access to key targets. The implemented strategy effects are similar to nationally-sponsored identity theft except using the breach method to support government endorsed options. A national cyber element could obtain third-party credentials, trace accounts, and close personal finance options until behavior changed while maintaining communication channels for conflict resolution. Acknowledging CES acts may benefit sanctioning powers through allowing negotiations while altering regional perceptions. Sponsored government digital

[61] Individual assets may be frozen but the author prefers leaving them within either a locked account or transferred to a holding location rather than disseminated. The outright removal of an individual's property may violate international law even with proper sanctioning.

[62] Rep. Cruz (TX), "Ensuring Lawful Collection of Hidden Assets to Provide Order Act." *Congressional Record* 163: 20, (Feb. 6, 2017) p. S873, Rep. Brooks (AL), "EL CHAPO Act." 115 Congress, 1st Session (2017)

communication would manipulate available venues to transmit desires and terms through controlled channels. If available retail systems are insufficient to support effective sanctions, PoS or similar authentication systems within government websites and networks offer additional breach options.

Breach's real advantage occurs in the intentional wealth redistribution made possible through owning data access. Once shares or accounts are controlled through cyberspace, the sanctioning nation could repurpose those funds to international requirements. The U.S. Congress stated in its House Resolution 499 that Russia should stop using coercive economic measures against the Ukraine and other regional countries.[63] This allows a potential interpretative expansion where those funds should be returned to the Ukraine. Here, the U.S. could adjust financial flows directly rather than wait for Russian government officials to compensate the Ukraine for damages. Data control could avoid the delays experienced in waiting for post-conflict financial resolution with unwilling partners.

Another breach option emerges from studying the sophisticated cyber-attack suffered by the Dutch digital certificate company, DigiNotar. Certificates, a digital financial transaction staple, are essential to secure internet interchange. Digital certificates guarantee three key functions; website authenticity, email, file and programming authenticity and integrity, and confidentiality through public key encryption. DigiNotar's firm was hacked on 10 July, 2011 and false certificates generated. The attack was

[63] Rep. Royce (CA), "Condemning the Violation of Ukrainian Sovereignty, Independence and Territorial Integrity by Military Forces of the Russian Federation." *Congressional Record* 160: 40, (March 11, 2014) p. H2268-73

discovered 19 July and false certificates revoked during initial mitigation. Public notice occurred 28 August and more false certificates, 531 in total, were discovered and mitigated. On 20 September, less than ninety days later, DigiNotar filed for bankruptcy, the firm's integrity irreparably damaged.[64] Manipulating certificates by challenging authenticity, preventing security, or infecting systems with secondary malware could prove vital to coercing sanctioned individuals by manipulating functional abilities and perceived reputations.

DigiNotar's breach used syntactic options and information functionality to manipulate secure communication methods. Simultaneously, the manipulation pulled the economic rug from beneath regional, digital commerce for targeted actors. Manipulation affected DigiNotar and individual's digital certificates and could function similarly through CES. Broadly modifying certificate vendor permissions could camouflage CES breach attempts against sanctioned individuals. One example would be selecting a wide customer list for apparent action when only certain individuals, like the thirty-one Russians indicated by the U.S. EO, warrant deeper influences.

As a theoretical example, a CES strategy using breach against certificates could prevent Bank Rossiya from accessing user data, denying some financial transactions while allowing other customers to use networked services. Certificate denial would acknowledge requested transactions without confirming authentication. Most users experience this when internet browser services prohibit connections due

---

[64] Nicole van der Meulen, *DigiNotar: Dissecting the First, Dutch Digital Disaster*, [6 No. 2] J. OF STRATEGIC SEC. 46, 47-49 (2013).

to unrecognized certificates or mismatched protocols. Individual certificates can be compromised further through additional techniques. Duplicating individual certificates could freeze accounts, transfer property, or generate additional accesses. Certificates fill a dual-role as both a known strength and a vulnerability within financial systems. The DigiNotar hack used this vulnerability to ruin the company as a side benefit of hacking their certificates. All transactions requiring certificates could be selectively affected including; blocking future financial exchange, bill payments, internet shopping, and potentially disabling secure communication. These interruptions could be effective when employed versus senior leaders in Russia, Crimea, or Russian-backed Ukrainian rebels relying on secure communications.

2. Disruption

One example of disruption techniques through DDoS appears against several U.S. bank chains. The Iranian-based Izz ad-Din al-Qassam Cyber Fighter's (QCF) group has conducted cyberspace disruptions against U.S. banks since 2012. Sanctions mirroring QCF behaviors could target identified Russian corporations like the Bank Rossiya. Since September 2012, QCF employed DDoS attacks against multiple U.S. banks including Bank of America, Wells Fargo, US Bank, JP Morgan Chase, Sun Trust, PNC Financial Services, Regions Financial, and Capital One as a supposed retaliation for an anti-Islamic video.[65] QCF is

[65] Emilio Iasiello, *Cyber Attack: A Dull Tool to Shape Foreign Policy*, NATO, 5th International Conference on Cyber Conflict, 1-18 (2013). From https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf

tentatively associated with Iranian and Palestinian groups but continues to publicly deny explicit origins.[66] US enforcement has not conclusively, or publicly, confirmed QCF's origin.

QCF attacks are tentatively attributed to Iran with no formal US indictments. Deceptive techniques disguising QCF's origins likely prevent policy makers from retaliatory actions. CES techniques may conceal effect origins or sanctioning individuals may acknowledge disruption attempts. Any Bank Rossiya or Chernomorneftegaz CES effort could be publicly declared, for example, to highlight international solidarity against a recalcitrant Russia. Declared events may be more effective but also will increase interstate tensions.

QCF attacks strike semantic and syntactic vulnerabilities.[67] Most attacks simply deny customer website access while approximately 25% attempt application layer strikes. Syntactic strikes against applications are disguised in larger attacks and incapacitate a banking infrastructure's web-servers.[68] Syntactically-based server incapacitation could disrupt a bank's long-term functionality. Technique effectiveness measurements should consider attack volume rates or secondary scans showing customer accesses to banking web portals during disruptive strategies. Sanctioning actors should be able to determine how

[66] Matthew J. Schwartz, *Threat Intelligence Can Rebuff DDos Attacks*, Information Week, Apr 22, 2013: 12.

[67] Semantic refers to website defacement and disruption while syntactic references software vulnerabilities.

[68] Robert Lemos, *Large Attacks Hide More Subtle Threats in DDos Data*, Dark Reading, May 18, 2013. From https://www.darkreading.com/analytics/security-monitoring/large-attacks-hide-more-subtle-threats-in-ddos-data/d/d-id/1139783

disruptive CES should be modified to achieve success.

QCF's DDoS techniques do not physically destroy banking capability or intellectual capital but change access volumes and influence customers. QCF's offensive suite included the highest volume DDoS functions at the time, at 70 Gigabits and 30 million packets per second. Security experts note banking corporation's larger infrastructures require increased attack rates for success.[69] High data rates may disguise other intended targets in overall transaction noise levels and allow additional actions. Sanction enhancement strategies using DDoS could include specific individual accounts and targeted corporations. As a potential CES shortfall, undeclared DDoS could be attributed to coincidental criminal action rather than intentional, international influences.

Manipulating QCF, or other DDoS techniques could prevent sanctioned industries from conducting digital transactions. Some industries will only be minimally affected while financial or foreign exchange corporations will see immediate impacts. DDoS functions could slow or stop transactions in generating targeted economic effects. QCF-like techniques could scale to first impede, then hamper, and finally to disrupt digital businesses. Impeded economic functions could include; payroll, banking, ordering, supply, and others essential to large corporations. All functions relate to core sanction elements by denying networked financial operations.

3. Functional Denial

A third CES technique examines Russian methods unveiled during the Georgian conflict by denying cellular

[69] Iasiello. "Cyber attack" 2013.

phones or other services to individuals or corporations. Modern digital lifestyles allow individuals to automate regular bill payments and disrupting these payments disrupts associated services. Effects first appeared as secondary results, and similarly denying phones, cable, internet, or even basic utilities could be effective against sanctioned entities. In August 2008, the Russian Army invaded Georgia and conducted the first, acknowledged, large-scale combined cyber and conventional attack. The two-phased attack began with a 7 August, Russian cyber-strike against Georgian government websites before cyber-targets expanded to financial institutions. Phase one employed semantic DDoS attacks with syntactic options to overwhelm Georgian servers. Denying government availability during the initial Russian invasion demoralized the Georgian populace and prevented effective command and control. Russia's phase two targets featured more extensive DDoS and struck Georgian politician's public-facing email accounts.[70]

Some potential CES techniques emerged in the conflict's second phase. Banking strikes decoupled financial systems from international networks and crippled dependent systems through denying automatic payment avenues; Automatic Teller Machine (ATM) systems, mobile phones with direct deposit, and other assets were all denied.[71] The Georgian cyberspace response was to accept temporary information losses and transfer most information assets to

[70] Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, [91 No. 6] MILITARY REV. 63-64 (2011).

[71] Marian Lazar (2012). The Russian Cyber Campaign Against Georgia (2012). In *The Complex and Dynamic Nature of the Security Environment*, 500-506. Bucharest, Romania: National Defense Univ., 2012.

neutral third party, geographic locations such as Poland, Estonia and the U.S.[72] Though physically separated, geographic isolation without network separation does not reduce CES impacts. Information movement did not prevent all of the Russian denial actions in Georgia as localized disruptions continued. CES employment would intentionally deny a sanctioned actors' financial accounts to prevent automatic payment, causing individual decision maker stress, and seeking broader impacts against Russian corporations. The overall CES intent remains shifting Russian national calculus on Ukrainian-associated decisions. Minimizing collateral impacts would allow some network functionality, even in sanctioned systems. Shifting accounts to other servers or nations could occur although cyber techniques can follow targets across geographic barriers.

Mirroring Georgian techniques could form a sanctioning state bot-net as an allied offensive network. The technique appears similar to the QCF scenario while being more easily attributable. A state wishing to publicly confirm their cyberspace options may select this option. Imagine a botnet horde, semantically altering all Bank Rossiya sites to post, "Bank Rossiya has been internationally sanctioned for supporting an illegal invasion by the Russian government against a sovereign state" or other, similar messages. Denying phone lines could minimize secondary effects to the local population who use associated services. Finally, controlling Global Cyber Commons access through network manipulation may allow information regarding crisis

[72] Col. Stephen W. Korns, *Botnets Outmaneuvered: Georgia's cyberstrategy disproves cyberspace carpet-bombing theory* ARMED FORCED JOURNAL (Jan. 1, 2009) Retrieved June 3, 2017 from: http://armedforcesjournal.com/botnets-outmaneuvered/

resolution to be transmitted to sanctioned decision makers.

4. Global Denial

The most impactful CES technique would be global denial. This technique strives to prohibit any digitally supported financial activity, globally, for the sanctioned entity and, for the time being, remains theoretical. There are no demonstrated public methods to support this means. Developing accesses and tools supporting global denials would be time and resource intensive. One envisions entering identifying characteristics within applications to use botnets, worms, or other methods thereby temporarily preventing financial functionality for a network or individual. Modern sanction systems notify banks, review accounts and deny transactions through regulation. Cyber tools would aim to prevent sanctioned individuals from completing any digital transactions, globally. For Russia, global CES denial would block all sanctioned individuals and corporations from completing any digital transaction for non-humanitarian purposes. Funds could be identified and tracked to prevent sanctioned individuals from disguising or transferring assets away from sanctioned techniques. One common sanctioning state concern is that blocked states sometimes no longer possess negotiation channels. Digital enforcement methods may allow communication channels like email or text to remain open despite physical blockades in other areas. These guaranteed channels would allow crisis resolution attempts or further sanction threats to be communicated securely and completely. Ensured digital communication channels could verify message transmission and reception to intended parties. CES allows sanction actions and negotiating resolution in the same, interdependent channel with guarantees provided through

cyber tools to ensure messages are transmitted and received by the intended party in some cases. The channel created to deny financial actions to the sanctioned party, could also be used to transmit to blockaded individuals. For example, think if Stuxnet had left messages inside Iranian systems suggesting which actions were required before centrifuge damaging, cyber activity was turned off by the initial actor.

B. Political and Technical Limitations

CES offers a strong theoretical argument, however, serious limitations do exist including: escalation and redline perceptions, legal constraints, and technical shortfalls. Each limitation possesses potential for policy and operational challenges. However, considering challenges enables developing a well-rounded, foreign policy toolkit including CES.

First, many policy makers fear crisis escalation. An initial escalatory action in many wargames is described as cyber-conflict, which increases or causes misunderstanding of redlines. Most politicians prefer not to see a soft power approach like CES degrade to unrestrained kinetic warfare. The same individuals fear expanding current cyber operations as they imagine all cyber-tools expanding past implanted controls similar to organic viruses. Despite common organic analogies, viruses and bacteria are much more sophisticated than cyber tools and more likely to adapt to new environments than manmade and constrained, cyber techniques. Current U.S. policy allows kinetic combat actions with relatively minor approval processes within declared Combatant Commander Areas of Responsibility. National cyber-tools remain much more tightly controlled than kinetic weapons despite the difference in scope. A 2,000-lb. bomb can be employed against a wide target

variety while cyber tools effect only a unique operating system, application or user. Transferring a constrained cyber method to another system could be considered similar to cross-species, organic virus transmission, possible but not likely. As mentioned earlier, covert operations still require congressional notifications and Presidential findings before action. Required cyber implementations approvals frequently limit offensive cyber techniques to previously approved military actions or require a Presidential finding for covert action. No U.S. government has publicly endorsed offensive cyber methods outside of either of these kinds of military actions.[73] Uncertainty regarding expressed cyber policy or escalation potential may impact U.S. decisions on CES means.

Another escalation element involves perceived international cyber redlines. Redlines provide operational and policy limitations to U.S. actions including those in cyberspace. Policy makers may be disinclined to add cyber provocations to tense diplomatic environments. Libicki argues for probabilistic versus determinist redlines in showing how varied trigger points allow more actor flexibility.[74] Probabilistic elements utilize declared lines, like "if you cross the border, we will respond". Determinist redlines suggest aggregated activity standards for situational responses, like "if you cross the border with a battalion, we may respond, or we may wait for additional actions and respond later". This variability creates monumental

---

[73] Catherine Theoharry & Anne I. Harrington, *Cyber operations in DoD policy and plans: Issues for Congress* Congressional Research Service R43848 at 16 (2015).

[74] Martin C. Libicki, *Two, Maybe Three Cheers for Ambiguity*, in CONFLICT AND COOPERATION IN CYBERSPACE: THE CHALLENGE TO NATIONAL SECURITY, by Panayotis A. Yannakogeorgos & Adam B. Lowther, 27-34 (2014).

difficulties when evaluating how the Russian government would respond to CES supporting the Ukraine. Evaluating state redlines should be no different than any other sanction although policy makers will require time to adapt to new domains like cyberspace. One can think of the first CES action as similar to the Cuban Missile Crisis, one knows new tools are available, but not how the other will use them. Adaptation will require similar timelines to when national strategies incorporated nuclear deterrence models, full-spectrum operations, and smart power techniques. CES success will likely go far to change hearts and minds on cyber-weapon employment.

Next, legal constraints pose potential limitations. Operationally, policy makers will require demonstrated planning showing how CES techniques meet U.S. laws, LOAC considerations, and UN guidelines. Any involved allies may pose additional constraints. As seen during Operations ALLIED FORCE and UNIFIED PROTECTOR, sometimes NATO partners have additional restrictions on appropriate responses. Kinetic actions require legal review before implementation and CES will likely require qualified lawyers evaluating options. The constantly changing restrictions and sheer volume of U.S. law make it impossible to consider even a fraction of potential alternatives here. However, the case study examines published U.S. policy and potential CES techniques in the Ukrainian crisis.

Third, technical shortfalls exist in the accesses and tools needed to affect digital networks. In simpler terms, one needs the door key, the knowledge of what is behind the door, and the capability to manipulate the underlying environment. Cyber tools have significant intelligence requirements for use, especially within restrictive environments like government networks or private digital accounts. Cyber-attacks require established access into

targeted systems and networks. Access provides the right path to manipulate a network and requires substantial intelligence prior to implementation. Each previous technique category highlighted known accesses and vulnerabilities. Intelligence operations need to recognize, discover and manipulate potential gaps before CES employment.

Possessing the right tool is not the only limiting factor. Cyber-associated intelligence agencies typically develop accesses for intelligence value and may not want to burn those accesses for sanction effects. Developing access for CES strategies requires a different focus and possibly organic access control by associated agencies. Coordinating access development and control across multiple agencies remains an issue for additional discussions. Obtaining timely access may be initially challenging but still likely faster than the decades one could spend enforcing ineffective Cuban and Iranian sanctions.

Associated with access is the difficult task of understanding how and where cyber techniques can be applied. Successfully attributing incoming cyber-attacks remains as challenging for defenders as discovering original vulnerabilities and accesses for attackers. Websites and tools offer penetration tips in both white-hat and black-hat applications. The most effective CES techniques may use microforce influences to disrupt or deny an individual's information accesses prior to affecting national decision calculus. All proposed techniques begin with finding a small vulnerability while ultimately affecting large activity swathes. In modern international relations, cyber vulnerabilities in corporations or leadership channels appear as common as finding national economic trade options for traditional sanctions. Individual effects require careful planning to prepare a selected network for desired outcomes.

Planning will also help minimize secondary and tertiary effects on the broader population. Resource investments should not vary greatly between large scale effects and individual sanctions.

After obtaining access and evaluating vulnerabilities, one must have the proper tool available. Cyber-weapons are difficult to stockpile usefully and predictably. The techniques above suggest where options exist although all will require design modifications before use. Starting with disruption, all presented techniques were narrowly targeted based on objectives. CES techniques require the same focus. The next crisis' necessary cyber-tool may not be the one employed previously. Cyber restricted employment comparisons to kinetic options shows the benefit and disadvantages when managing government acquisition needs against future crisis. However, cyber offers the only reversible weapons in modern history. The theory, proposed by Rowe et. al, advocates releasing only cyber-weapons whose effects may be reversed once a desired impact is achieved.[75] In the Ukraine, one could impact the multiple individuals mentioned and remove those effects as desired actions occur. This method blends neatly with targeted sanctions by removing any damage once all parties reach an agreement, unlike kinetic strikes destroying command structures. These technical limitations may seem initially daunting but are no more so than similar tactical and technical challenges faced during either the Combined Bomber Offensive or the Apollo Program. Just like those concerns, resources and national desire will likely help solve

[75] Neil C. Rowe, *et al. Challenges in Monitoring Cyberarms Compliance*, in CONFLICT AND COOPERATION IN CYBERSPACE, by Panayotis A. Yannakogeorgos & Adam B. Lowther, 81-99 at 92, (2014).

this problem.

IV. A UKRAINIAN CASE STUDY

CES uses cyber means to improve financial sanction effectiveness in achieving U.S. national ends. The suggested strategies above are applied here to the recent Ukrainian crisis. CES complements U.S. policy by implementing economic sanctions against individual and corporate actors to manipulate international decision-making calculus through microforce applications. The cyberspace domain's unique advantages allow CES to apply pressure differently than traditional sanctions. Techniques affecting governmentally sanctioned entities already exist in the public cyber domain. Increasing economic sanctions overall effectiveness without incurring national costs in either tangible, such as military blockades, or intangible, such as public image, areas is a valuable diplomatic tool. The case presented here allows U.S policymakers to verify the CES guidance, standards, and application employed as well as projected effectiveness in the Ukraine crisis.

This case examines how U.S. policy sets cyber guidance, what regional conflict standards exist, how CES techniques may be applied, and what effectiveness metrics are needed. First, guidance evaluates whether sufficient state controls exist to impose cyber sanctions. Most guidance emerges from public policy statements, legislative acts, or national decrees. Second, standards are assessed by determining possible and effective CES methods against cyber techniques already employed regionally. Third, and potentially the most controversial section, several CES strategies are suggested. As a strategic look, even though discussing techniques, this area is hypothetical since no tool modeling conducted against regional networks has occurred.

Finally, CES effectiveness metrics are only suggested because implementing any new action can be difficult if one does not know where national success may lay in any particular case. No sanction can succeed without positively changing the decision calculus involving the sanctioned state. These areas suggest how CES extends current policy and highlights how cyber means increase sanction effectiveness in one scenario.

A quick crisis background is essential for proper orientation. The regional crisis began late 2013 over whether Ukrainian international trade agreements should be European-focused or maintain a Russian preference. The traditionally Russian aligned Ukrainian government clashed with their people before President Yanukovych and his supporters fled the country on 21 February 2014. Immediately after, a Ukrainian political coup on 27 February 2014 completed the political transition to a European-centric focus and activists from both pro-Ukrainian and pro-Russian sides took to the streets to protest as neither side was content. The most severe clashes between the pro-Ukrainian and pro-Russian groups initially occurred in the Crimean province.

On 1 March 2014, Russian President Vladimir Putin received parliamentary approval to invade the Ukrainian regions and deployed troops charged with protecting Crimean-based ethnic Russians. On 16 March, Crimea held a provincial referendum and overwhelmingly voted to join Russia with a 96% voter turnout and over 80% of the populace voting for secession. Although the Ukraine, the U.S., the European Union and several other nations denounced the vote as illegal, Russian President Putin annexed Crimea the following day.[76] The U.S. and the

[76] Steven Woehrel, *Ukraine: Current Issues and U.S. Policy*, at 4, Congressional Research Service, (2014).

European Union have levied numerous sanctions while diplomatic attempts at formal conflict resolutions continue. Ongoing activity shows border conflicts, Russian support for separatists inside Ukrainian territory, and no apparent crisis resolution in the near term. The Ukrainian conflict provides a useful framework to show how a CES could be employed inside of current national guidelines. Attempting to influence Russian decision making through CES begins with understanding what U.S. national leadership's ends are for the Ukrainian crisis.

A. CES Guidance

When employing CES, one should first consider whether national guidance appears sufficient to develop clear ends. U.S. guidance regarding Ukrainian sanctions is sufficient to implement clear objectives for the following reasons: (1) US Executive Orders govern sanction policy in the region, (2) the Department of Treasury's published guidance implementing sanctions are detailed down to the individual, (3) U.S. legislation including congressional actions and Executive Orders define the Ukraine as a national security interest. US Executive Orders (EO) govern sanction policy within the Russian region. Presidential EO and the DoT's Office of Foreign Asset Control (OFAC) expansions sanctioning Russia is sufficiently directive to generate microforce options, suggest accesses, and direct priorities for CES planning and employment.[77] The multiple

[77] Department of the Treasury. UKRAINE AND RUSSIA RELATED SANCTIONS http://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx (last visited June 3 2017).

EOs issued by President Obama identified those forces undermining Ukrainian stability and integrity as an emerging US national security threat. Four orders, EO 13660, EO 13661, EO 13662, and EO 13685 are currently published on the current crisis with each addressing slightly different categories.[78] The first three highlight Ukraine while EO 13685 addresses Crimea. The orders identify both individual and corporate actors with a range from politicians and generals to banks and factories. The description's breadth includes categorical guidance to sanction those who contribute to Russian military efforts. The broad guidance would allow further sanctioning activity against almost any Russian economic industrial function.

EO guidelines clearly define initial sanctions, though depend on OFAC development for additional emphasis

[78] The first order, issued 6 March 2014, declares restraints on persons identified by the Secretary of Treasury and State, within five categories, as contributing to Ukrainian unrest. The second EO, issued on 16 March, continues to expand, and provides four more categories including Russian government officials and arms merchants. The second EO further identifies seven Russian government individuals directly as sanction targets. The third EO provides three more categories, but highlights any individual operating within Russian Federation economic sectors including: financial services, energy, metals and mining, engineering, defense or related material. The description's breadth allows almost any Russian economic industrial function to receive sanctions. All EOs order any property and interests currently residing within the US, transferred later or within control of any US person blocked and states they, "may not be transferred, paid, exported, withdrawn, or otherwise dealt." THE AMERICAN PRESIDENCY PROJECT *Blocking Property of Certain Persons Contributing to the Situation in Ukraine*, Exec. Order No. 13660, 79 Fed. Reg. 46 (March 10, 2014); THE AMERICAN PRESIDENCY PROJECT, *Blocking Property of Additional Persons Contributing to the Situation in Ukraine*, Exec. Order No. 13662. 79 Fed. Reg. 56 (March 24, 2014).

points. No individuals were immediately identified by OFAC after publishing the initial EO. After the second EO, four more actors were identified for sanction by OFAC in addition to naming seven other actors through annexes. Following the third EO, 20 more individuals and Bank Rossiya were identified by OFAC as sanctioned entities. As Ukrainian events continued to degrade through 2014, seven additional Crimean individuals and a Crimean gas and oil exploration company, Chernomorneftegaz, were sanctioned. The OFAC's Sanction's Program, has developed a Sectoral Sanctions list to identify all individuals available for sanction through at least physical addresses.[79] Other information associated with listed individuals includes: name and aliases, date and place of birth, and official positions. Corporate identities feature: names, physical addresses, web addresses and emails. All information can be supplemented by intelligence sources once a CES strategy is implemented

The provided descriptions highlight the opportunity for CES in the Ukrainian conflict. U.S. policy identifies individuals and corporations who are sufficiently distinct from others to meet at least LOAC definitions, if not other international law requirements. Cyber operators, following Presidential guidance, could use multiple techniques against individuals, corporations, or government agencies. Individual, identifying characteristics will allow techniques to use narrow effects or manipulate entire networks. The recent SCADA attacks against the Ukraine in 2015 demonstrated their network vulnerabilities.[80] The details

[79] Office of Foreign Assets Control, http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (accessed April 15, 2014).
[80] Robert M. Lee *et al., Analysis of the Cyber Attack on the Ukrainian Power Grid*, (2016).

sufficiently distinguish between sanctioned individuals and potentially innocent victims.

U.N. sanctioning processes prefer to notify affected and sanctioning governments before implementing sanctions. A request for exception to U.N. due process and prior notice rules appears within section 7 of all currently referenced EOs. This section 7 exception states the U.S. will begin sanctioning activities without notifications as early action U.S. legislation supports the EOs desire to act without prior notification. The guidance here is H.R. 4152, *To Provide for the costs of loan guarantees for Ukraine*, passed on 3 January 2014, and states US policy as, "to use all appropriate economic elements of US national power, in coordination with US allies to protect the independence, sovereignty, and territorial and economic integrity of Ukraine"[81] Another relevant Act HR 4278, the Ukraine Support Act, explicitly refers to sanctions and passed the House on 27 March 2014.[82] This House bill became S2183 in the Senate and a part of public law in April 2014.[83] HR 4278 specifically provides sanction guidance both complementing published EO and expanding their scope. The most recent bill introduced was HR 830, "Stability and Democracy for Ukraine" which shows a continued desire in

[81] Rep. Rogers (KY) *Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014*, 22 U.S.C. 8901, Apr. 3, 2014, P.L. 113-95 (113th Congress), H.R. 4152.

[82] Sen. McConnel (KY), *United States International Programming to Ukraine and Neighboring Regions*, 22 U.S.C. 6211, Apr. 3, 2014, P.L. 113-96 (113th Congress), S.2183, H.R.4278 [introduced by Rep. Royce (KY)].

[83] Sen. McConnell (KY) *United States International Programming to Ukraine and Neighboring Regions*, S. 2183, Apr 3. 2014, P.L.113-96 (113th Congress).

section 201 to prohibit financial transactions with Russia, and reaffirms the previously mentioned Executive Orders.[84] The guidance extracted from U.S. Presidential EO, DoT actor development, and existing US legislation demonstrate sufficient guidance to implement CES against potential vulnerabilities within the Ukrainian conflict.

B. CES Standards

The next strategic step would assess regional standards through analysis of currently employed cyber techniques throughout the region. LOAC proportionality means using minimal force and employing similar methods. Standard cyber techniques used by either Russia or the Ukraine will likely limit how CES techniques are employed. Detected methods may legally justify equivalent U.S. CES techniques against Russia. Simply put, if Russia introduced cyber-weapons into the conflict against the Ukraine, such as the 2015 and 2016 SCADA attacks, no legal reason exists why the U.S. and allied nations should not use CES techniques to resolve the conflict.

One cyber-weapon weakness regards whether a tool can be captured and reprogrammed to affect original users. Part of the Ukrainian, and U.S., risk is whether Russian cyber expertise is sufficient to subvert CES techniques and redirect them. Ukrainian cyber activities suggest no new strategies are being introduced although, at the tactical level, several new applications have appeared. Since 7 March 2014, the Ukrainian conflict has included publicly recorded cyber events on both sides.

---

[84] Rep. Engel (NY) *Stability and Democracy for Ukraine Act*, H.R. 830, 115th Congress, 1st Session (2017).

Initially, on the Ukrainian side, the pro-Ukrainian Kibersotnya group's attacks directly defaced Russian news websites with Distributed Denial of Service (DDoS) techniques.[85] Connection through the top-level public and private websites were blocked by the defacements. Non-specific but Ukrainian associated hackers have claimed to have rerouted links, stolen data, and compromised passwords. DDoS attacks prevented individuals from reaching government sites in order to deny support and direction during the crisis. Initial FSB attribution credits multiple Ukrainian hackers with defacements without a final judgment.[86] Overall, both identified techniques influenced a wider spectrum than this CES proposal, probably due to the overall directional lack underlying the Ukrainian cyber effort. CES's disruption, breach, and functional denial techniques all appear within Ukrainian cyber activity.

On the Russian side, a pro-Russian group, Cyber Berkut, used DDoS tools against NATO and Ukrainian media websites. Cyber Berkut initiated attacks after NATO's public statement denounced Crimea's independence

---

[85] Government and Commercial systems included the Russian presidential website, Central Bank of Russia, Ministry of Foreign affairs and the energy consortium Gazprom.

[86] *The Ukrainian Crisis - A Cyber Warfare Battlefield*, OSNET Daily. April 10, 2014. http://osnetdaily.com/2014/04/the-ukrainian-crisis-a-cyber-warfare-battlefield/ (accessed April 11, 2014). The FSB, Federal'naya Sluzhba Bezopasnosti, or Federal Security Service, was created from the largest remaining element of the KGB after the dissolution of the Soviet Union. Originally focused only on counterintelligence, they have since assumed other duties and function as a national intelligence agency for Russia. Andrei Soldatov, & Irina Borogan, *The Mutation of Russian Secret Services*, Argentura.ru. 2011, http://www.agentura.ru/english/dosie/mutation/ (accessed May 3, 2014).

referendum and deployed personnel to Kiev.[87] A second local hacktivist group, Anonymous Ukraine (AU), appears in cyber activity dating back to November 2013. In May 2014, AU released intercepted emails between a US Army Attaché and a senior Ukrainian Army Official coordinating for potential U.S. aid and support.[88] Again, one sees the prevalence for broad activity rather than targeted events coordinated within a central plan. Other government emails were likely included in the interception. The email intercept shows government officials within both conflicting parties and outside entities as validated vulnerabilities. Russian disruption and breach techniques mimic the same proposed CES options.

One regionally unique cyber-attack does appear with a named infiltration. Regional security filters detected a Russian military cyber espionage tool, known as Snake or Ouroboros, throughout Ukrainian information systems. Snake implantation allows operators complete network access but may include as yet undetected clandestine destructive options. Some cyber techniques can conceal additional microforce techniques against specific systems within the overall code. Stuxnet demonstrates where a tool designed for information gathering also affected centrifuge operations. Since 2010, fifty-six Snake infections occurred globally with thirty-two Ukrainian networks overall, and twenty-two since January 2014.[89] Undetected infections

---

[87] Matthew J. Schwartz, *DDoS Attacks Hit NATO, Ukrainian Media Outlets*, DarkReading. March 17, 2014. http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742 (accessed June 4, 2017).

[88] *Id.*

[89] Sam Jones, *Ouroboros: Cyber Snake Infects Ukraine Computer Networks*, FINANCIAL TIMES, (Mar 7, 2014).

could be much wider. Snake mimics the CES suggested breach technique.

The broadest Russian event was the attack on Ukrainian power systems during the December 2015 to January 2016 period. The event consisted of a hacker attack on multiple Ukrainian corporations with the goal of disrupting power distribution in the short-term. This was the first recorded attack conducted against a SCADA system to specifically prevent power distribution. Sandworm, a Russian-backed hacker group, used Black Energy 3, a malware tool, to infiltrate business systems and then digitally move from those systems to field sites where actual power distribution was influenced.[90] The hackers likely began reconnaissance six to nine months prior to the actual attacks. The attack ultimately blocked power to 225,000 customers over several hours.[91] Also noted was KillDisk malware use to delete information from infected computers and slow the recovery processes.[92] The same software, Black Energy 3 and KillDisk, was also noted during the same timeframe on a Ukrainian mining company and a large railway operator.[93]

---

[90] Danika Blessman, *Black Energy Malware is Back and Still Evolving*, (2016) https://www.solutionary.com/resource-center/blog/2106/01/black-energy-malware (last accessed June 4, 2017).

[91] Robert M. Lee *et al.*, *Analysis of the Cyber Attack on the Ukrainian Power Grid.* (2016).

[92] Symantec Security, *Destructive Disakil Malware Linked to Ukraine Power Outages Also Used Against Media Organizations*, (2016) https://www.symantec.com/connect/tr/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations?page=1 (last accessed June 4, 2017).

[93] John Leyden, *Black Energy Trojan Also Hit Ukrainian Mining Firm and Railway Operator*. (Feb. 15, 2016)

Both Ukrainians and Russians have deployed cyber tools regionally. Choosing cyber methods means both parties seek domain influences to favorably affect the conflict's eventual resolution. Selected and confirmed cyber targets to date include government websites, banks, and personal emails. All will likely continue to appear on future vulnerability lists. Additionally, both short duration influences and longer-term infiltrations are present. LOAC analysis suggests CES appears proportional with the existing techniques. In a broader sense, CES may be more humanitarian than infantry attacks or no-fly zone enforcement. U.S. CES implementation is well within overall legal and regional standards. Both standards and guidance sections favorably support CES employment.

C. CES Techniques

While discussed above in greater detail, CES techniques for breach, disruption, functional denial, and global denial are suggested here as strategic options. Specific vulnerabilities are referenced from above sections. This element covers how each item could alter the conflict and lead to rapid resolution. Actual implementation will rely on developed tools and accesses, most likely outside of public discussion channels. After all, fully identifying tools and vulnerabilities prior to use helps defenders patch those same channels.

The first implemented technique should be breach. Much as with the Snake technique above, breach methods

---

http://www.theregister.co.uk/2016/02/15/blackenergy_trojan_trend_micro (last accessed June 4, 2017).

introduce all sanction accesses. Breach techniques generate accesses and intelligence to increase later effectiveness. Studies, such as the one by Aaltola et. al., demonstrate methods patterning networked activities through the global commons and show potential vulnerabilities.[94] CES strategies could use techniques to rapidly create multiple accesses across wide-ranging regional systems. Multiple breach methods could generate increased data and minimize mitigation by local cyber-security due to confusion and complication. Breach should be publicly denied and minimally impactful on system performance to maximize the tool's lifespan in affected systems. Examples of breach successes could be used during negotiations to demonstrate potential power.

If breach alone is insufficient to reduce a crisis, disruption attempts could be introduced. The discussed DDoS methods do not require internal network access but only external port awareness. As seen with QCF attempts against U.S. banks, increasing the overall traffic for corporations can reduce digital transactions. The available bot-net size, strength, and tool sophistication will drive overall effectiveness. Disruption can affect OFAC designated individuals by reducing their ability to coordinate government efforts. In-person meetings may, of course, still occur while reduced internet access, especially across large areas will slow Russian government response times.

Once breach or other methods generate sufficient access, if further escalation is required, functional denial can be used to prevent Russian individuals and corporations from conducting activities. Combining phone service functional denial with internet disruption as in the Georgia

[94] Mika Aaltola *et al.*, *The Challenge of Global Commons and Flows for US Power*, (2014).

example will prevent coordinated Russian responses. Functional denial should also strive to decouple corporations from their international financial channels. Most large corporations, especially the Russian oil and gas corporations, depend on international income. This method, paired with analysis, can identify sanctioned individual and corporate accounts to digitally separate the funds. Once separated, funds may be transitioned to generate Ukrainian humanitarian aid, restore the stolen accounts in HR 4152, or any other financial relief.

Finally, CES global denial, if tools and vulnerabilities are available, would eliminate Russian access to any cyberspace options. Other than specific white-listed options to encourage communication and resolution, removing internet access within a modern society could generate significant impacts. Initial implementation should only deny labeled sanctioned individuals. Subsequent deployment could reach OFAC suggested, rather than specified, Russian targets. Implementing global denial would remove the need for either disruption or functional denial but is potentially more difficult to implement.

Operational means surely exist to employ all developed CES strategies in the Ukrainian crisis although whether any nation also possesses the desire to employ these techniques is a separate question. Each method suggests where targets are available and implementation can be conducted while limitations including access and tool availability were discussed earlier. Further, once implementation occurs, it will be important to understand where Russian redlines exist. Redlines may cover how fast, and to what degree CES can be implemented without impacting non-cyber areas. As a technical alternative, in each area, CES methods provide expanded options to implement an already approved sanction regionally rather

than merely preventing Russian access to U.S. and EU accounts through traditional means as occurs today. In many cases, these funds may already be undervalued or difficult to reach. Expanding sanction options logically means regional pressure will increase and may drive more expedient conflict resolution. Overall, sanction effectiveness rests not within the specific techniques but in altering national decision calculus.

D. CES Effectiveness

CES employment goals are interrupting financial flows without humanitarian impact to affect national decision calculus. CES effectiveness means impacting sanction enforcement to drive conflict resolution quicker, at lower cost, and with less negative humanitarian impact than traditional sanction enforcement or military options. Since traditional sanction timelines can be measured in decades, projected cost over time versus a faster resolution with CES is an important effectiveness consideration. Since CES has not been implemented anywhere, no quantitative data exists to support potential cost savings. However, all sanctions evaluate three qualitative effects after implementation; (1) does the sanctioned state begin or continue useful discussions with the implementer, (2) does depriving resources shift regional power, and (3) whether increased sanctions are required. State negotiation involvement is a binary measurement even if diplomatic teams can add various qualitative standards. Diplomatic discussions requesting sanction abatement may also indicate success. Additionally, functional denial or breach may impact individual negotiators who will be measured through their participation or communications passed through white-hat CES channels. National intelligence services may also

uncover specific, individual impacts, and reduce uncertainty volumes regarding future conflict resolution negotiations.

Effectiveness measures should relate how implemented CES changes negotiations between the targeted state and the implementing country. Currently, the U.S. continues discussions with Russia regarding the Ukraine but no conflict resolution is imminent. Some Treasury metrics can be employed to assess status. These measures may include how many resources were employed to achieve sanction effects versus the reduction in financial power to sanctioned entities through trade volume, direct investment, or national economic products. Although not a total measurement, when Russia invaded the Ukraine on 1 March 2014, a ruble was worth .02775 U.S. Dollars (USD). One year later, one ruble was worth .01638 (USD), a drop of just over 40% demonstrating a significant loss in individual purchasing power. The lowest point over the same interval was .1435 (USD) but the ruble does appear to have stabilized at between .17 and .18 (USD) during April to June 2015.[95] Even those numbers still show a 30% comparative decrease. Prior to the 1 March date, over the past ten years, the Russian ruble had only closed lower against the dollar over a several day span in February 2008.[96] Not directly attributable to sanctions, similar or additional metrics could show increased effectiveness for CES. Public statements reflecting on sanctions can be measured by frame and discourse style analysis to assess CES's regional power impacts. Data to measure all areas can emerge from national intelligence

[95] XE.com."RUB/USD chart" http://www.xe.com/currencycharts/?from=RUB&to=USD&view=2Y (accessed June 4, 2017).
[96] *Id.*

services, trade reports, media publications, or other social sources.

Shifting regional power can be measured either quantitatively or qualitatively. Russian military deployments can be tracked through both measurements. CES effectiveness metrics could track order of battle intelligence and supplies delivery to determine whether funds exist to move military units in the affected area. Social media and news interviews can show both equipment supply rates and morale for troops at economically depressed locations. Supply chain statistics from sanctioned corporations may also be measured. If leadership decides to shift funds directly to opposition groups; both transfers and end-user effectiveness with those funds can be evaluated by trade volume and secondary effects. For example, funds held by Leonid Slutsky, a State Duma Deputy identified in the 16 March EO, could be used for the desire expressed in HR 4152 sec 3.9 to support Ukrainian Government efforts, "to recover and return to the Ukrainian state funds stolen by former President Yanukovych..." and others. Effectiveness could be measured through either funds removed, or funds returned to the Ukrainian state as a percentage of the overall totals reported stolen. Breach, disruption, functional denial, and global denial methods all assist in providing relevant data to improve sanction effectiveness.

The final effectiveness question assesses whether increased sanctions are likely to achieve desired effects. This assessment is forward looking through using behavioral trends. Measurements may be scaled regarding state political shifts referencing particular positions. Both intelligence sources and media reporting will inform planners regarding increased sanction necessity. In Russia, some sources may highlight discrepancies between original, international agreements and subsequent actions. One example is the

punitive trade measures Russia has imposed on Ukraine, Moldova, and Georgia.[97] These show how Russia has tried to alleviate the gap in their own finances through punitive tariffs on neighbors. Scaling future CES or other sanctions to influence emerging situations will largely depend on the sanctioned countries' perceived responses. For the Ukraine, policy makers will likely set timelines for scaled Russian responses such as government statements, actions like withdrawing troops or establishing weapons cantonments, and full crisis resolution. If timelines are not met, additional sanctions can be undertaken. When timelines are met, cyber effects can be quickly reversed. CES generates increased effectiveness during scaling because since techniques allow escalation, or reversal through altering coding. It is much easier to undo an IP address within code than rebuild a fallen bridge. Reversibility within traditional sanctions can be similarly slow. One important policy consideration will be how many resources are required to scale CES effects. Specific metrics to measure CES effectiveness in each situation will also require further development.

V. CONCLUSION

Cyber Enhanced Sanctions are not merely more cyber-warfare methods but a strategic attempt to bring new tools into international relations. Planners have sought to implement targeted sanctions for twenty years by purely diplomatic measures but cyberspace microforce effects may tip the balance. Some limitations exist regarding willpower,

---

[97] Denis Cenusa, *et al*, *Russia's Punitive Trade Policy Measures towards Ukraine, Moldova and Georgia*, Centre for European Policy Studies Working Document 400, September 2014.

legality, or tools and access but most can be alleviated through discussion and planning. Even legal questions can be addressed through constructivist activities in normative construction such as those used when accelerating President Obama's drone war.[98] If limitations are mitigated, CES will expedite effects compared to traditional sanctions by bringing the opposing state to the bargaining table, shifting regional power balances, or threatening increased sanctions.

The examined areas demonstrate where CES has applicability and will likely improve conflict resolution within the Ukraine. Existing guidance clearly demonstrates how CES could be applied within the scenario. Standards show where CES fits within international legal guidance and regional standards. Technique implementation demonstrates specific areas where CES will improve national power means. Finally, the effectiveness summary demonstrates how CES strategies can be measured against commonly regarded sanction metrics, if implemented. All examined areas show where CES could improve financial sanctions applications within this crisis. From the Ukrainian standpoint, CES is a tool that policy makers should consider examining for inclusion within the smart power toolkit.

CES strategies may provide ways to improve financial sanction effectiveness in achieving national power ends. Cyber suggests precise options are possible while meeting nebulous financial and political guidelines and still remaining inside international legal standards and other agreements. Traditional sanctions are difficult to employ and may require a decade's long commitment without achieving significant effects. In today's interdependent world, being

[98]Jeffrey Lantis, ARMS AND INFLUENCE: U.S. TECHNOLOGY INNOVATIONS AND THE EVOLUTION OF INTERNATIONAL SECURITY NORMS, (2016).

able to apply effects across multiple channels and alter those effects to dynamic situations is an invaluable tool. Similar to this method are other common debates such as identifying cyber-weapons through block-chain techniques or tool signatures. Effective sanctions in today's connected environment requires learning new means; cyber techniques may offer those solutions, or at least, expanded options.

The continuing Ukrainian dispute with Russia demonstrates an international crisis where financial sanctions, as they exist today, seem incapable of reaching a resolution within a reasonable time. Ongoing hardships for the Ukrainian people will only be resolved by forcing Russia's hand to end the conflict. Smart power options generated through CES strategies and cyber employment offers expanded opportunities. Developing and implementing Cyber Enhanced Sanctions in accordance with published policy and legislation will increase economic sanction effectiveness. Publicly available tools demonstrate several fundamental approaches including: breach, disruption, functional denial, global denial, or combinations of the same. All techniques could be modified for emerging policy and capability restraints or planned as wholly new options.

One of CES's most appealing options to any leader should be the available malleability including identifying specific actors, reversing effects, and whitelisting secure communication channels. These benefits allow national leaders to scale sanctions to fit every developing crisis rather than being a cookie-cutter tool. In addition to scaling, these cyber enhancements will allow some mid-level, sanctioned leaders to negotiate without navigating national hierarchies, potentially avoiding their leadership and crafting alternative solutions.

CES benefits should, in time, make this option an essential component in any national economic strategy through increasing overall sanction effectiveness. Improved effectiveness occurs in three areas: generating increased intra-state discussion opportunity, shifting regional power between internal players and providing expanded options when required. Thirty years of implementing minimally effective Iranian sanctions and Russian leaders continuing to ignore current US sanctions clearly means additional tools are badly needed as part of the U.S. toolkit.

CES allows sanctions, on political leaders, to be adjusted dynamically rather than waiting for regulatory and legislative action. Cyber-enhanced Sanctions (CES) demonstrate the potential means to increase financial sanction effectiveness and achieve national ends without committing costly or politically sensitive military forces. CES should be the first power step for the U.S. in any foreign crisis requiring sanction. Even if military forces have the only expertise to support CES, it will still be better than the massive financial and physical commitments required for conventional wars in distant lands or non-effective traditional sanctions. CES strategies may generate substantial and measurable success for national policy makers without decade-long commitments to sanctions or boots on the ground. In sum, implementing Cyber Enhanced Sanction strategies with the discussed guidelines and potential techniques appears both possible and effective in the near to mid-term as an option in the U.S. foreign policy toolkit.