Penn State Journal of Law & International Affairs

Volume 5
Issue 1 *War in the 21st Century and Collected Works*

April 2017

The Cyber Longbow & Other Information Strategies: U.S. National Security and Cyberspace

Gary D. Brown

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

THE CYBER LONGBOW & OTHER INFORMATION STRATEGIES: U.S. NATIONAL SECURITY AND CYBERSPACE

*Gary D. Brown**

* Gary D. Brown is a retired U.S. Air Force Judge Advocate. He served as U.S. Cyber Command's first senior legal counsel.

TABLE OF CONTENTS

I. INTRODUCTION

The U.S. is struggling to effectively contest its adversaries in cyberspace. It would seem natural for the U.S. to be the leader in every aspect of internet operations, after all, the internet was invented in the U.S., and the U.S. is dominant in many areas. However, there are regions of cyberspace in which the U.S. is not the leader, perhaps because of a misapprehension about the nature of cyberspace.[1]

This paper will provide a definition of cyberspace suitable for national security strategy discussions and address how the U.S. should approach cyberspace operations to engage its adversaries in the most effective manner. Historically, the U.S. has been a champion at leveraging soft power. Cyberspace has become an essential way to increase the reach and penetration of soft power, yet the U.S. appears on some levels to be losing in cyberspace to non-state groups like ISIS and to other State actors such as Russia.

This paper suggests that it would be more effective to think of cyberspace as a combination of infrastructure (the internet) and the information and ideas that move across the infrastructure (the ideosphere, as defined below). This model of cyberspace helps increase the emphasis on engaging with the actors and information using the internet in ways counter to U.S. national interests.

II. BACKGROUND

Cyberspace is an unprecedented national security challenge. It doesn't align with standard U.S. government organizational constructs, which are generally either geographic or defined by specific functionality. Although it is hosted on physical infrastructure that has a physical location, it's often not helpful to think of cyberspace in geographic terms. Additionally, it's not straightforward to characterize it functionally because cyber capabilities support every

[1] At least one author rejects the notion that cyberspace can even have a nature. This may reflect the definitional problem discussed below. *See* Lawrence Lessig, *Code and Other Laws of Cyberspace (1999).*

agency and activity, and enable adversary activities, as well as being the primary focus of some adversary missions.

U.S. strategy seems to put less emphasis to acting on information, rather, focusing on the physical elements of cyberspace.[2] Concentrating on the hardware and operating systems – basically the internet – rather than other elements of cyberspace requires confronting specific operational issues. The internet is, well, the internet.

Disabling or destroying hardware in one location may have transnational effects. It can raise sovereignty concerns for allies and others, and restrict the ability of the U.S. to operate, in addition to compromising intelligence equities. Perhaps most vexing though, disabling or destroying hardware raises questions of how to attribute those activities to individual actors. Engaging on *content* rather than *infrastructure* can limit these issues. To some extent the U.S. has begun to realize this, undertaking at least some discussion about engaging ISIS on both its ability to use the internet to communicate, and about changing the communications to alter the message.[3]

Infrastructure-focused strategy also represents a lost opportunity. Cyber operations aren't a particularly good method for asserting national interests directly because of the ancillary effects set out above, and because they tend to be packets of boutique capabilities that don't easily translate to large-scale operations. However, cyberspace is an ideal medium for the exercise of soft power.[4] Spreading ideals of freedom of speech, economic principles, and democratically-driven culture, for example, supports U.S. national security interests. As noted below, U.S. adversaries have

---

[2] *Infra.*

[3] Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N.Y. TIMES (Apr. 24, 2016), http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=1.

[4] Soft power is the ability to get what you want through attraction and persuasion rather than coercion or payments. It arises from the attractiveness of a country's culture, political ideals, and policies. Joseph S. Nye, Jr., *Soft Power* (2004) [*hereinafter* "Nye"], pp. 5-8.

been more effective at using this aspect of cyber power to maximize their interests, which often run contrary to those of the U.S. The U.S. should do more to close this divide.

III. RIVAL APPROACHES TO CYBERSPACE

Although the U.S. is skilled in cyber activity, its focus has been on espionage and, to a lesser extent, on military activity aimed at disrupting or damaging internet infrastructure. Focusing on cyber infrastructure for non-intelligence operations has placed the U.S. behind some of its rivals in important aspects of cyberspace. Set out below are three examples of approaches to the strategic use of cyberspace that largely focus on the content rather than the infrastructure, along with suggestions regarding how the U.S. might glean lessons from each.

A. China

The modern Chinese economy was built on commercial espionage.[5] The Chinese government has even gone so far as to formalize the strategy of stealing intellectual property to advance its economy, developing a branch of the PLA, Unit 61398, dedicated to cyber espionage. By stealing industrial secrets to advance its economic might, China is following a strategy modeled in the early days of the U.S. The U.S. has protested, but it is hard to ignore the historical irony of the situation. It was national policy in the early days of the American republic to acquire European technology by any means available, a policy that resulted in the U.S. emerging as the world's industrial leader.[6] For example, in 1789 Samuel Slater emigrated to the U.S., bringing with him an intimate knowledge of the Arkwright spinning frames that had transformed textile

[5] Joshua Philipp, *Hacking and Espionage Fuel China's Growth*, EPOCH TIMES (Sept. 10, 2015), http://www.theepochtimes.com/n3/1737917-investigative-report-china-theft-incorporated/.

[6] Doron Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power* (2004); Alexander Hamilton, *Report on the Subject of Manufactures* (Dec. 5, 1791), http://www.constitution.org/ah/rpt_manufactures.pdf.

production in England. Using this knowledge, Slater set up the first water-powered textile mill in the U.S. Two decades later, the American businessman Francis Cabot Lowell talked his way into a number of British mills, and memorized the plans for the hi-tech Cartwright power loom.[7]

The U.S. and China agreed in 2015 not to engage in commercial espionage against each other, but there is doubt China will uphold its end of the bargain. If China violates the agreement the U.S. government may respond with economic and political action, but there is little that can be done by the U.S. to directly prevent Chinese commercial espionage. Attempts to defend against espionage have been less than completely successful. The U.S. government could respond in kind, stealing intellectual property and other commercial information from China through cyberspace – although U.S. industry is generally advanced compared to Chinese industry – so that course of action provides little gain.

For the U.S., the closest effective equivalent to Chinese action might be to remove the barriers for private citizens to strike back with cyber means as a response to being victimized by this type of action. Often called "hacking back," many companies have expressed frustration with ineffective government action in the area, and noted a willingness to use their own cyber expertise to retrieve stolen data, render it unusable, or simply to punish perpetrators by disrupting their networks. Government officials consistently note the dangers in this type of action.[8] If the U.S. decided to change course and allow self-help activity, it would have to consider amending several statutes prohibiting unauthorized access to both computers and data, at rest and in transit.[9] However, there seems to be little

---

[7] James Surowiecki, *Spy vs. Spy*, THE NEW YORKER (Jun. 9 & 16, 2014), http://www.newyorker.com/magazine/2014/06/09/spy-vs-spy-3.

[8] Craig Timberg, Ellen Nakashima & Danielle Douglas-Gabriel, *Cyberattacks trigger talk of 'hacking back*,' WASH. POST (Oct. 9, 2014), https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.

[9] These statutes include the *Computer Fraud & Abuse Act (CFAA)*, 18 U.S.C. §1030; the *Electronic Communications Privacy Act*, 18 U.S.C. §§ 2510-2521 and the *Stored Communications Act*, 18 U.S.C. §2701. CFAA, in particular, is considered by

appetite for this in Washington, and the U.S. has aggressively pursued criminal action for what might be seen as relatively minor violations of computer security statutes.[10]

B. ISIS

A non-state actor that has been active in cyberspace is ISIS.[11] ISIS has been successful at using social media to promote its message of violence and recruit members. Al Hayat, ISIS' media department, has released carefully choreographed, ideology-focused videos that have been called "Jihadi infomercials."[12] These videos present a message encouraging would-be Jihadists and foreign fighters to answer the call of duty. The videos feature foreign fighters appealing to their brothers to reject Western values and join the fight. This message provides a strong moral pull, appealing to the estranged and isolated, particularly in Western Europe and in the U.S.

ISIS spreads its message using a variety of social media, the most popular being Twitter and web forums. As ISIS advanced in its territorial acquisitions, it posted pictures of hundreds of massacred Iraqi soldiers on Twitter. The photos inspired horror and fear, which appeared to be the intended result. ISIS videos of beheadings and executions have been posted for maximum visibility. In a YouTube video uploaded in August of 2014 an Iraqi police chief was beheaded. His head was placed on his legs, and ISIS tweeted the picture with the words, "This is our football, it's made of skin." The photo included the hashtag #WorldCup, causing it to pop up in the news

---

some to be overly broad. *See* Electronic Frontier Foundation, https://www.eff.org/issues/cfaa.

[10] Mark Jaycox & Lee Tien, *Obama's Computer Security Solution is a Mishmash of Old, Outdated Policy Solutions*, ELECTRONIC FRONTIER FOUNDATION (Jan. 16, 2015), https://www.eff.org/deeplinks/2015/01/obamas-computer-security-solution-mish-mash-old-outdated-policy-solutions; Doe, *FBI raids dental software researcher who discovered private patient data on public server*, DAILY DOT (May 27, 2016), http://www.dailydot.com/politics/justin-shafer-fbi-raid/.

[11] The Islamic State in Iraq and Syria (ISIS) is also referred to as IS, ISIL, and Daesh.

[12] Jesse Singal, *Why ISIS Is So Terrifyingly Effective at Seducing New Recruits*, N.Y. MAGAZINE (Aug. 18, 2014), http://nymag.com/scienceofus/2014/08/how-isis-seduces-new-recruits.html.

feeds of those following the hugely-popular soccer tournament in Brazil, ensuring millions of views.[13] ISIS also has foreign recruits use their personal Facebook and Twitter pages to report positive experiences about the movement, posting pictures of themselves apparently living wealthily in extravagant houses, showing the material upside to joining ISIS.[14]

The U.S. has tried to engage on social media, but at least with publicly disclosed programs, it has generated more embarrassment than success.[15] As a nation, the U.S. has generally been good at using soft power, even if it most often has been a happy byproduct of American business success rather than a planned government activity. During the Cold War, for example, East Germans were able to listen to American punk rock and dissident announcements on *Radio Glasnost*, which was run by private citizens.[16] This was an example of combining the natural attractiveness of Western culture with the power of private citizens to tailor the narrative to suit U.S. national security goals.

---

[13] Tomlinson & White, *This is our football, it's made of skin #World Cup: After posting sickening beheading video of Iraqi policeman, ISIS boast of slaughtering 1,700 soldiers*, DAILY MAIL (Jun. 13, 2014), http://www.dailymail.co.uk/news/article-2656905/ISIS-jihadists-seize-two-towns-bear-Baghdad-U-S-tanks-helicopters-stolen-fleeing-western-trained-Iraqi-forces.html.

[14] Deborah Richards, *The Twitter jihad: ISIS insurgents in Iraq, Syria using social media to recruit fighters, promote violence*, AUSTRALIA BROADCASTING CORPORATION (Jun. 20, 2014), http://www.abc.net.au/news/2014-06-20/isis-using-social-media-to-recruit-fighters-promote-violence /5540474.

[15] Such as trumpeting the decision to deploy more U.S. troops to Iraq when that is one of the primary concerns of Muslims in the region. Elizabeth Cohen & Debra Goldschmidt, *Ex-terrorist explains how to fight ISIS online*, CNN (Dec. 21, 2015), http://www.cnn.com/2015/12/18/health/al-quaeda-recruiter-fight-isis-online/.

[16] Esme Nicholson, *The Cold War Broadcast That Gave East German Dissidents a Voice*, NPR (Nov. 8, 2014), http://www.npr.org/sections/parallels/2014/11/08/361160675/the-cold-war-broadcast-that-gave-east-german-dissidents-a-voice. Radio and television from West Germany was quite effective at educating East German audiences on the benefits of the non-Communist world. Esther von Richthofen, *Bringing Culture to the Masses: Control, Compromise and Participation in the GDR* (2009), p. 103.

The diverse population of the U.S., the production and international distribution of films and television programs, American domination in the music and sports scenes, and the availability of U.S. higher education to foreigners have all helped build an impressive machine for the U.S. to wield soft power.[17] Although this may not translate directly into advancing U.S. national interests, it does show the potential for spreading U.S.-based information effectively. This attraction to popular cultural has helped the U.S. achieve important foreign policy goals, such as reconstruction after WWII and victory in the Cold War.[18]

Unfortunately, the relative ability of the U.S. to project soft power seems to have diminished in the past several years. The U.S. has reduced its credibility in the Middle East by engaging in multiple conflicts there and demonstrating little cultural understanding.[19] The internet-enabled lower barrier to entry for news channels and information distribution has increased competition for the attention of the masses, and decreased the ease with which the U.S. can project its values. Official outlets in other States are more trusted by foreign countries, while U.S. official outlets are less trusted abroad than unofficial U.S. outlets.

To regain its soft power mojo, the U.S. must evolve, learning to use information to its advantage. It's easy to see, for example, how some stories could present a favorable contrast between the adversary's cause and Western values, e.g., reportage on ISIS killing male European jihadists who arrive in theater, and subjecting females who arrive to sexual slavery.[20] There is some hope on this front, as

---

[17] Nye, *supra* FN. 4, at Chap. 2.

[18] Nye, *supra* FN. 4, at 49-53.

[19] President George W. Bush's announcement of the "war on terror" and call for democratization of the Muslim world, for example, failed to engage with the local population and damaged U.S. soft power reserves. Nye, "The Future of Soft Power in U.S. Foreign Policy," in *Soft Power and US Foreign Policy* (2010), pp. 4-7.

[20] Nadette de Visser, *ISIS Eats Its Own, Torturing and Executing Dutch Jihadists. Or Did It?*, DAILY BEAST (1 Mar. 2016), http://www.thedailybeast.com/articles/2016/03/01/isis-eats-its-own-torturing-and-executing-dutch-jihadists-or-did-it.html; Sam Webb, ""A living hell': The grim fate that awaits British teenage girls

the U.S. Secretary of State met with Hollywood executives to discuss the impact on groups like ISIS of how the U.S. is portrayed in movies.[21]

In the absence of an effective U.S. government response to terrorist successes in cyberspace, and under pressure to do *something*, private companies have begun to step up their game. Notably, Google has developed a capability to redirect searches for terrorist information to pre-existing anti-terrorist material on YouTube.[22] It's too early to determine how effective the program will be.

This issue remains on the radar of strategic thinkers in the U.S. government, as well. Recently, the State Department began a new campaign to help slow recruitment efforts from extremist groups like ISIS. For example, under the new campaign, the U.S. has been shifting away from directly sending messages to potential ISIS recruits through the Center for Strategic Counterterrorism Communications (CSCC), as it proved to be ineffective.[23] The CSCC approach was ultimately abandoned after being reviewed by a team comprised of non-governmental individuals. The reviewers undoubtedly observed that it wasn't very effective to counter an organization that operates under the notion that Western governments are illegitimate with official statements from one of

believed to be joining ISIS," *Mirror* (Feb. 21, 2015), http://www.mirror.co.uk/news/uk-news/a-living-hell-grim-fate-5203372.

[21] Ryan Faughnder, *John Kerry meets with Hollywood studio executives to talk Islamic State*, L.A. TIMES (Feb. 16, 2016), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-john-kerry-hollywood-isis-20160216-story.html.

[22] Jack Detsch, *How Google aims to disrupt the Islamic State propaganda machine*, PASSCODE (Sept. 7, 2016), http://www.csmonitor.com/World/Passcode/2016/0907/How-Google-aims-to-disrupt-the-Islamic-State-propaganda-machine?cmpid=ema:nws:Daily%2520Newsletter%2520%2809-07-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160907_Newsletter:%20Daily&utm_term=Daily.

[23] Executive Order 13584, *Developing an Integrated Strategic Counterterrorism Communications Initiative* (Sept. 9, 2011); Simon Cottee, *Why It's So Hard to Stop ISIS Propaganda*, THE ATLANTIC (Mar. 2, 2015), http://www.nationaldefensemagazine.org/archive/2016/April/Pages/USProceedingwithNewStrategy toCounterISIL.aspx; Hayes Brown, "Meet The State Department Team Trying To Troll ISIS Into Oblivion," *Think Progress* (Sept. 18, 2014), http://thinkprogress.org/world/2014/09/18/3568366/think-again-turn-away/.

those governments. One of the reviewers noted that "'it's not the U.S. government that's going to break the [Islamic State] brand. It's going to be third parties.'"[24]

Reloading, the Department of State has now created the Global Engagement Center (GEC), which is designed to enable partners in countries with a majority Muslim population to act as messengers, rather than the State Department delivering information directly.[25] The GEC is supposed to be the single entity in charge of coordinating social media engagement to counter terrorist organizations like ISIS. It promises to engage in "rigorous research and modern data analysis" as well as "create, develop and sustain effective positive alternative narratives consistent with U.S. policy objectives."[26] Unfortunately, while these are appropriate objectives, they seem inconsistent with maintaining rapid-fire engagement like that undertaken by motivated individuals supporting ISIS, who appear to receive little guidance from higher headquarters, but have managed to control the narrative.[27]

Favorable facts must reach the targeted populations quickly to make a difference, however: "Falsehood flies, and the Truth comes limping after it."[28] Information programs encumbered by a cautious bureaucratic process will never be timely enough to make much of a difference. Crowdsourcing appears to be superior to government in every aspect of internet engagement.[29] However, it is

---

[24] Greg Miller, *Panel casts doubt on U.S. propaganda efforts against ISIS*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/world/national-security/panel-casts-doubt-on-us-propaganda-efforts-against-isis/2015/12/02/ab7f9a14-9851-11e5-94f0-9eeaff906ef3_story.html?postshare=901449106173651&tid=ss_tw.

[25] E.O. 13721, *Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad* (Mar. 14, 2016), http://www.jurist.org/documents/executiveorders/13721.php.

[26] *Id.*

[27] Philip Kapusta, *The Gray Zone*, SPECIAL WARFARE (Oct.-Dec. 2015 (p. 22), http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf.

[28] Attributed to Jonathan Swift (1710).

[29] Ariana Eunjung Cha, *What Yelp can tell you about a hospital that official ratings can't*, WASH. POST (Apr. 5, 2016), https://www.washingtonpost.com/news/to-your-health/wp/2016/04/05/going-to-the-hospital-read-the-yelp-reviews-first/.

not clear that the State Department understands the importance of nongovernmental involvement.

An additional issue with government agencies disseminating information involves the restrictions setforth in the *Smith-Mundt Act,* which prohibits the domestic distribution of public diplomacy information.[30] *Smith-Mundt* has been interpreted broadly inside the government as prohibiting the dissemination of information by means that *might* be seen by Americans.[31] This creates a difficult standard when the material is online and anyone in the world could potentially see those materials. The federal government shouldn't be attempting to influence U.S. audiences, but when this type of guidance is broadly interpreted it ignores the reality of cyberspace. The result renders U.S. information efforts impotent and cedes the field to terrorists who then control the narrative, unopposed.

Even though *Smith-Mundt* was amended in 2013 to address this issue, it remains unclear how the law will be interpreted going forward.[32] There appears to be residual resistance to distributing information by cyber means because of the potential exposure of American citizens.[33] As a fully realized democratic society, the U.S. is especially concerned about maintaining a reputation for truthfulness in the government. That is not true of every U.S. competitor.

---

[30] Matt Armstrong has written extensively on *Smith-Mundt*, for example at *Smith-Mundt Modernization Act of 2012 Introduced in House*, MOUNTAINRUNNER (May 17, 2012), https://mountainrunner.us/2012/05/smith-mundt-modernization-ac/.

[31] It's unclear at this point whether or when practice will change to match the change in the law.

[32] Mick West, *Debunked: 2013 NDAA Thornberry amendment, domestic propaganda, disinformation*, METABUNK.ORG (May 21, 2012), https://www.metabunk.org/debunked-2013-ndaa-thornberry-amendment-domestic-propaganda- disinformation.t592/.

[33] Nafeez Ahmed, *Your Government Wants to Militarize Social Media to Influence Your Beliefs*, MOTHERBOARD (Nov. 14, 2016), http://motherboard.vice.com/read/your-government-wants-to-militarize-social-media-to-influence-your-beliefs.

C. Russia

The Russians are masters of using cyberspace to advance their information agenda. Russia leverages disinformation on an industrial scale, for example, by spreading misleading claims about Sweden's stockpiling of nuclear weapons, stating that nuclear weapons on a Turkish base were at risk, by persistently denying the presence of Russian troops in Ukraine, and most recently, by leading a misinformation campaign during the 2016 U.S. presidential election.[34] In addition, they have been comfortable allowing, even encouraging, private citizens to engage in offensive cyber activities when they coincide with national interests.[35]

Russia's willingness to engage the private sector in this fashion is one reason that it has been able to remain at the forefront of cybersecurity operationally and diplomatically. Other States have been less willing to take this step. In fact, despite Russia's success with this tactic, the U.S. and other Western countries do everything they can to prevent private actors from engaging in offensive cyber activities. This is reminiscent of continental Europe's reaction to England's mastery of the 14th century's super-weapon, the longbow.

England adopted the use of the longbow early in its history. From the beginning, it was clear the longbow's range and penetration power was superior to those of other weapons of its time. Longbows put crossbows to shame, being only a fraction of the cost, with a much greater firing speed and range. It was a perfect, inexpensive

---

[34] Neil MacFarquhar, *A Powerful Russian Weapon: The Spread of False Stories*, N.Y. TIMES (Aug. 28, 2016), http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=1; Shane Harris, "Clinton Foundation: Those *Hacked Files' Aren't Ours,* DAILY BEAST (Oct. 4, 2016), http://www.thedailybeast.com/ articles/2016/10/04/clinton-foundation-those-hacked-files-aren-t-ours.html; *U.S. was reportedly more prepared for Russian cyber attacks than disinfomation campaign*, REUTERS (Dec. 20, 2016), https://venturebeat.com/2016/12/20/u-s-was-reportedly-more-prepared-for-russian-cyber-attacks-than-disinformation-campaign/.

[35] *See* Allen & Leeson, *infra* note 33; Levi Maxey, *Cyber Proxies: A Central Tenet of Russia's Hybrid Warfare*, THE CIPHER BRIEF (Feb. 24, 2017), https://www.thecipherbrief.com/article/tech/cyber-proxies-central-tenet-russias-hybrid-warfare-1092.

weapon for peasants, as it was basically a stick of wood. Masses of peasants armed with longbows were so critical to the defense of the realm that Edward I prohibited all manner of sport among the peasantry except archery, and Edward III made weekly archery practice obligatory, banning other forms of competing activities.[36] Henry VIII compelled longbow ownership and also prohibited activities that competed with the mandatory longbow practice.[37] The result of making archery the only lawful recreational activity for decades was a large mass of superbly capable "special forces" available to the king. England's domination in this field was complete.

England basically maintained its monopoly on longbow use for one hundred and fifty years. This wasn't because wood and peasants were in short supply elsewhere, nor because other rulers didn't know how effective the longbow was, but because other kingdoms lacked the political stability to trust such a powerful weapon in the hands of the rabble.[38] England was favored with the political stability that gave it confidence to encourage a talented and armed population. The opportunity to "crowd-source" longbow techniques and skills significantly improved England's military capability. Currently, Russia is employing a similar strategy in the case of hacking skills.

Although it may not be the most stable State in the world, Russia has enough national coherence that it has allowed a number of private citizens to practice with powerful cyber tools. Russia's level of comfort with its political stability and unity has allowed it to leverage the power of private citizens to perfect the use of a powerful weapon. This hasn't given Moscow a monopoly on cyber weaponry, but has provided a different element to its cyber strategy, meriting

---

[36] Douglas W. Allen & Peter T. Leeson, *Institutionally Constrained Technology Adoption: Resolving the Longbow Puzzle*, THE J. OF L. & ECON. (2015) [*hereinafter* "Allen & Leeson"] p. 683, 688, http://www.peterleeson.com/Longbow.pdf.

[37] Allen & Leeson, p. 689.

[38] England's longbow dominance lasted from about 1332-1428. Allen & Leeson, pp. 683-684.

comparison with the English longbow model.[39] Cyber criminals are allowed to hone their hacking skills and their hacking tools, using both for the advancement of outward-directed criminal enterprises. Russia allows this broad access to a powerful means of warfare, resulting in the development of a trained cadre of cyber operators with ever-improving tools. While Russia must accept the inherent risk that this cyber capability could be turned against the regime's interest, it can also avail itself of this force when the nationalist sentiment can be employed to in advance State interests. The Kremlin is in a position to purchase the loyalty of these groups by acquiescing in the commission of cyber crime, creating a shared interest.[40]

In addition to leveraging patriotic feelings and private cyber expertise, Russia actively manipulates social media for its national security purposes, both internally and abroad. For example, people are hired to post negative comments about anti-Russia articles online, and do the opposite for pro-Russia articles, with the intent to overwhelm rational discourse on Western media sites.[41] These Russian professionals have also used Twitter falsely to report an oil spill and an Ebola outbreak in the U.S., perhaps testing a capability to manipulate public opinion and create confusion and mistrust.[42] Even if these false messages reach only a relatively small number of people, social networks have an extraordinary power to convince people and manipulate opinion.[43]

---

[39] Trend Micro increasingly observes hackers' relationships with official authorities and their participation in conflicts. Max Goncharov, *Russian Underground 2.0*, TREND MICRO (2015), http://www.trendmicro.fr/media/wp/russian-underground-2-0-wp-en.pdf.

[40] Mathew J. Schwartz, *Russian Cybercrime Rule No. 1: Don't Hack Russians*, BANK INFO SECURITY (Sept. 14, 2015), http://www.bankinfosecurity.com/blogs/russian-cybercrime-rule-no-1-dont-hack-russians-p-1934.

[41] Daisy Sindelar, *The Kremlin's Troll Army*, THE ATLANTIC (Aug. 12, 2014), http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/.

[42] Adrian Chin, *The Agency*, N.Y. TIMES MAG. (Jun. 2, 2015), http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

[43] *The Social-Network Illusion That Tricks Your Mind*, MIT TECH. REV. (Jun. 30, 2015), https://www.technologyreview.com/s/538866/the-social-network-illusion-

The U.S. might learn from Russia's use of both social media and private actors. The distinction between the way ISIS uses social media and the way Russia does is that ISIS reports its activities, however mortifying they are, and attempts to spin its own situation to look enticing to recruits. Russia uses social media outlets to manipulate public opinion in ways that aren't apparent, and using means that aren't easily attributable to Moscow. There is evidence that U.S. companies manipulate the news to benefit their perceived interests, as well, so it isn't as if this technique is unknown inside the U.S., it just doesn't appear to be used by the government.[44]

Although the U.S. has been reluctant to employ the "cyber longbow" like the Russians have, there are plenty of examples of private citizens performing useful national security work merely as an unplanned collateral result of acts of conscience or activism. People around the globe have joined to oppose ISIS online, both as individuals and as part of groups like Ghost Sec.[45] Some are actively engaging; others are taking good citizen-type actions such as

---

that-tricks-your-mind/; Sean Gallagher, *Air Force research: How to use social media to control people like drones*, ARS TECHNICA (Jul 17, 2014), http://arstechnica.com/information-technology/2014/07/air-force-research-how-to-use-social-media-to-control-people-like-drones/.

[44] Michael Nunez, *Former Facebook Workers: We Routinely Suppressed Conservative News*, GIZMODO (May 9, 2016), http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006; Reena Flores, *Hillary Clinton Google suggestions accused of favoring candidate*, CBS NEWS (Jun. 11, 2016), http://www.cbsnews.com/news/hillary-clinton-google-suggestions-accused-favoring-candidate-election-2016/. As noted in the article, Google denies manipulating the results.

[45] Shashank Shekhar, *Desi hackers join cyber war on ISIS: 'Hacktivist' group Anonymous says 1,000 Indians are sniffing out jihadi Twitter accounts and websites*, DAILY MAIL INDIA (Nov. 25, 2015), http://www.dailymail.co.uk/indiahome/indianews/article-3334089/Desi-hackers-join-cyber-war-ISIS-Hacktivist-group-Anonymous-says-1-000-Indians-sniffing-jihadi-Twitter-accounts-websites.html; Jack Smith IV, *Anonymous Divided: Inside the Two Warring Hacktivist Cells Fighting ISIS Online*, TECH.MIC (December 04, 2015), http://mic.com/articles/129679/anonymous-vs-isis-how-ghostsec-and-ghost-security-group-are-targeting-terrorists#.tEWnKSnXD.

reporting Twitter accounts that support terrorist activities. Terrorist attacks in Paris motivated many online to strike back at ISIS.[46]

Individual actions aren't limited to opposing terrorist groups. Hackers have lashed out at China in support of pro-democracy protesters in Hong Kong.[47] The hacker group Anonymous released information about drug-related corruption in Mexico, after finding government action there ineffective.[48] Anonymous also decided to support protests in support of democracy in Hong Kong, taking down thirty government sites.[49] Additionally, a group called the Elves works to counter Kremlin trolls who spread propaganda and disinformation about Lithuania.[50] Child pornography has also become

---

[46] Andrew Blake, *#OpISIS and #OpParis: Anonymous hacktivists to retaliate against ISIS after Paris attacks*, WASH. TIMES (Nov. 16, 2015), http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/; Swati Khandelwal, "#ParisAttacks — Anonymous declares War on ISIS: 'We will Hunt you Down!,'" *Hacker News* (Nov. 16, 2015), http://thehackernews.com/2015/11/parisattacks-anonymous-isis.html; David Goldman & Mark Thompson, "Anonymous blocks jihadist website in retaliation for Charlie Hebdo attack," *CNN* (Jan. 12, 2015) http://money.cnn.com/2015/01/11/technology/security/anonymous-charlie-hebdo/.

[47] Mary-Ann Russon, *Anonymous brings down 30 Chinese government websites to support Hong Kong protesters*, INT'L. BUS. TIMES (Apr. 13, 2015), http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

[48] Rodrigo Bijou, *Governments don't understand cyber warfare. We need hackers*, TED (Dec. 2015), https://www.ted.com/talks/rodrigo_bijou_governments_don_t_understand_cyber_warfare_we_need_hackers/transcript?language=en.

[49] Mary-Ann Russon, *Anonymous brings down 30 Chinese government websites to support Hong Kong protesters*, INT'L BUS. TIMES (Apr. 13, 2015), http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

[50] Michael Weiss, *The Baltic Elves Taking on Pro-Russian Trolls*, DAILY BEAST (Mar. 20, 2016), http://www.thedailybeast.com/articles/2016/03/20/the-baltic-elves-taking-on-pro-russian-trolls.html. The group has been compared to the resistance fighters in the region during WWII.

a target of citizen hacker groups.[51] These are all indications that some, at least, see hacking as a legitimate form of citizen action.[52]

To emulate the success of the Russians, the U.S. may have to trust the public with the cyber longbow. Private companies have employed hackers to their advantage, even going so far as using such hackers in the fight against U.S. adversaries. There are some indications the U.S. government might permit private citizens with cyber capabilities to use them wisely in certain circumstances.[53] When the FBI was unable to access the iPhone of the terrorists who killed 14 people in San Bernardino, California – and Apple refused to assist – the Bureau reportedly paid hackers to accomplish the task.[54] The government has also shown signs it will work with hackers to advance national defense, with programs like "Hack the Pentagon," in which it offers a bounty to hackers who find and report vulnerabilities in DoD computer networks.[55]

---

[51] *Anonymous Hacktivist Group Now Gunning for Powerful Pedophile Networks*, SPUTNIK NEWS (Jan 26, 2016), http://sputniknews.com/europe/20150124/1017301478.html#ixzz48LNRiLjF.

[52] Lorenzo Franceschi-Bicchierai, *A Notorious Hacker Is Trying to Start a 'Hack Back' Political Movement*, MOTHERBOARD (May 23, 2016), http://motherboard.vice.com/read/notorious-hacker-phineas-fishers-is-trying-to-start-a-hack-back-political-movement.

[53] Katie Moussouris, *Hackers Can Be Helpers*, N.Y. TIMES (Mar. 30, 2016), http://www.nytimes.com/roomfordebate/2016/03/30/should-hackers-help-the-fbi/hackers-can-be-helpers; Nichole Hong, *U.S. Revamps Line of Attack in Social-Media Fight Against Islamic State*, WALL ST. J. (Aug. 28, 2016), http://www.wsj.com/articles/u-s-revamps-line-of-attack-in-social-media-fight-against-islamic-state-1472415600?utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20EBB%2008-29-16&utm_term=Editorial%20-%20Early%20Bird%20Brief.

[54] Shane Harris, *Did the FBI Just Unleash a Hacker Army on Apple*?, DAILY BEAST (Mar. 29, 2016), http://www.thedailybeast.com/articles/2016/03/29/did-the-fbi-just-unleash-a-hacker-army-on-apple.html; Kevin Pousen, *Double Cross*, WIRED (May 2016), https://www.wired.com/2016/05/maksym-igor-popov-fbi/.

[55] Statement by Pentagon Press Secretary Peter Cook on DoD's Hack the Pentagon, CYBERSECURITY INITIATIVE PRESS OPERATIONS (Mar. 2, 2016), http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

Of course, hackers tend to be independent thinkers and actors who have their own conception of right and wrong. One of the bigger challenges presented by these groups includes using their skills to interrupt lawful discourse. For example, groups have acted to prevent a candidate from running for public office and hacked a newspaper because it published information that they didn't agree with.[56] While it's certainly true that most private groups come with significant baggage, there simply is no substitute for crowdsourcing.[57] The opportunity to leverage the efforts of millions of people around the globe to invent, solve, and improve is perhaps cyberspace's greatest strength. No government effort can compete with the results of this type of massive collaboration over the long haul, even if it is as unsavory in its methods as hacking ISIS Twitter accounts with pornography.[58] And, surely no government agency would have rick-rolled ISIS, unleashing the devastating Rick Astley on potential ISIS recruits.[59]

The U.S. has tended to shy away from citizen groups like Anonymous because the groups' often offensive behavior, and, because they sometimes act against the U.S. government's perceived interests. Sometimes the obnoxious activities can't be ignored, but most hacker groups seem generally to be in favor of democratic rule and freedom, so there ought to be much common ground with the

---

[56] *Id.; Catalin Cimpanu, Anonymous Warns US Sen. Ted Cruz to Leave Presidential Race, or Else*, SOFTPEDIA (Mar. 21, 2016), http://news.softpedia.com/news/anonymous-warns-us-sen-ted-cruz-to-leave-presidential-race-or-else -502009.shtml; Waqas Amir, *Hacktivists Shut Down Donald Trump Hotel Collections Website*, HACKREAD (May 21, 2016), https://www.hackread.com/donald-trump-hotel-collections-website-down/.

[57] Dai Davis, *Hacktivism: Good or Evil?*, COMPUTER WKLY. (Mar. 2014), http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil.

[58] Jacob Bogage, *This hacker is fighting ISIS by spamming its Twitter accounts with porn*, WASH. POST (Jun. 14, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/14/this-hacker-is-fighting-isis-by-spamming-its-twitter-accounts-with-porn/?utm_campaign=Defense%20EBB%206-15-16&utm_medium=email&utm_source=Sailthru.

[59] James Geddes, *Hacking Group Anonymous Using Rick Astley Video to Rickroll ISIS*, TECH TIMES (Nov. 28, 2015), http://www.techtimes.com/articles/110795/20151128/hacking-group-anonymous-using-rick-astley-video-to-rickroll-isis-video.htm.

U.S. government. The benefits of exploiting the commonality could be enough to outweigh the negative. The general resistance to cooperating with the government creates an obvious barrier to working with hacker groups, and the challenges shouldn't be underestimated, but the potential is so great the government ought to make an effort. The U.S. should search for those areas of overlapping interests, subtly encouraging, or at least not discouraging, private action in these areas.

Russia appears to have found a way to keep the groups that it works with under control, and the U.S. must do likewise if it intends to make better use of this resource. Russia enjoys the benefit of working with groups motivated by money. Wealth is a straightforward way to secure the cooperation of these groups. Less concrete goals of groups like Anonymous – increased freedom? more free speech? – present a greater, but not insurmountable, challenge.

IV. A WAY FORWARD

One thing that might be preventing more creative U.S. national security activities in cyberspace is how the U.S government defines the actual term "cyberspace." Rethinking that definition should be the first step in any U.S. rebalancing efforts.[60]

The U.S. *International Strategy for Cyberspace* uses the terms "digital infrastructure" and "internet" throughout as stand-ins for cyberspace.[61] Similarly, the Department of Defense (DoD) defines cyberspace as, "A global domain within the information environment consisting of the interdependent network of information technology

[60] The word cyberspace is a bit of a historical accident. Novelist William Gibson is credited with coining the term. He wanted a "really hot name" to use in his novels, and recognized the value of cyberspace because it was evocative of much but "meant absolutely nothing." https://www.brainpickings.org/2014/08/26/how-william-gibson-coined-cyberspace/.

[61] *International Strategy for Cyberspace* (May, 2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[62] Both of these terms suggest an approach focused on the physical aspect of cyberspace, largely ignoring the people and thoughts (content) that make cyberspace important.

A more useful approach looks at cyberspace as "the internet plus the ideosphere." Taking the terms separately, the **internet** is the global communication network that allows computers to connect and exchange information, consisting of hardware such as servers, routers, cables, and switches, as well as the software necessary for the hardware to operate.

The **ideosphere**, on the other hand, is the "place" where ideas are created and grow. It's where thoughts and theories are made and evaluated.[63] As ideas interact, often instantly on a global scale only possible through cyberspace, they change form. The evolution of ideas is in some ways like the evolution of living organisms, but much faster. Ideas fuse, recombine, and evolve rapidly. The basic element of replication in the ideosphere is the meme, which serves in a role analogous to the gene in physical reproduction.[64] There are many aspects of the ideosphere, but it may be simplest to define it as "the universe of ideas."[65] It is here where U.S. adversaries excel, and, as a result, where the U.S. needs to focus.

If strategic thinking about cyberspace were guided by a framework of cyberspace as the internet plus the ideosphere, strategy would be less likely to focus on infrastructure, and more likely to concentrate on engaging with the content in cyberspace. Jim Lewis, Senior Fellow at the Center for Strategic and International Studies puts it this way, "The problem in the US is we're very militarized, so

---

[62] JP 1-02, DOD DICTIONARY (Feb. 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[63] Douglas Hofstadter, METAMAGICAL THEMAS: QUESTING FOR THE ESSENCE OF MIND AND PATTERN, 50 (1987).

[64] Google defines meme as "a humorous image, video, piece of text, etc. that is copied (often with slight variations) and spread rapidly by Internet users."

[65] Hofstadter, at 50-51.

we tend to think about attacking infrastructure. The Russian approach is much more political and about trying to manipulate public opinion."[66] A disadvantage of focusing on infrastructure is that everyone has an interest in keeping the internet functional, and that significantly limits engaging with the infrastructure itself.[67] It's the information and ideas that U.S. adversaries are using to their advantage, and information should be a priority for U.S. national security efforts. At least one U.S. ally has taken steps in this direction. Britain's NSA equivalent, GCHQ, apparently engages with terrorist internet content to discredit and embarrass leadership, in addition to issuing false orders to individual terrorists (or potential ones).[68]

Focusing engagement on content rather than infrastructure has the added benefit of avoiding one of the thornier problems of waging cyber-war – attribution. The U.S., for obvious reasons, seeks to avoid negative effects on infrastructure owned by its political allies. Information, on the other hand, can be weighed by reference only to the information itself. Sophisticated technical operations are required to determine whether engagement is appropriate. If information is helpful to an adversary it can be addressed regardless of the source and without effect on infrastructure.[69]

---

[66] Jack Detsch, *In aftermath of the DNC hack, experts warn of new front in digital warfare*, PASSCODE (Aug. 10, 2016), http://www.csmonitor.com/World/Passcode/2016/0810/In-aftermath-of-the-DNC-hack-experts-warn-of-new-front-in-digital-warfare?cmpid=ema:nws:Daily%2520Newsletter%2520%2808-10-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160810_Newsletter:%20Daily&utm_term=Daily.

[67] Taking down connected networks quickly decreases the utility of the other networks, as well. Metcalfe's Law states that the value of a network is proportional to the square of the number of users, a concept whose implications for military operations will have to be explored elsewhere.

[68] Forno & Joshi, *America is 'dropping cyberbombs' – but how do they work*?, THE CONVERSATION (May 11, 2016), https://theconversation.com/america-is-dropping-cyberbombs-but-how-do-they-work-58476?mc_cid=a6d6f926a2&mc_eid=3284b6aba6.

[69] Consistent with Constitutional protections, which tend to be applied to everyone regardless of nationality.

V. CHALLENGES

The First Amendment's guarantee of freedom of speech may be the single most important right that defines what it means to be an American.[70] A key component of the exercise of free speech is the ability to communicate freely without government interference. Distinguishing protected speech from impermissible speech will always be an issue in the U.S.[71] A particular complicating factor is that often, speech is permissible under some circumstances but not others. Fiction and satire are examples of vehicles that can protect normally unlawful speech. On the other hand, shouting "fire" when there is none could be a lawful (albeit not very funny) joke, but may be unlawful if that same joke resulted in injury or harm for people trying to escape the building in which the joke was made.

An illustration of how challenging putting all this together can be is Microsoft's policy on dealing with "terrorist content." Microsoft's approach includes definitions of prohibited speech (which includes ". . . endorses a terrorist organization or its acts …") and an exclusion for its search engine, which will still be allowed to return content responsive to searches for terrorist content.[72] For the government to engage aggressively to remove content that is damaging to national security (i.e., terrorist recruiting, lethal knowledge like bomb making skills, or offensive propaganda) it must find a way to determine when unpleasant or undesirable speech crosses the line from constitutionally protected to legally impermissible, based on content or context. Microsoft's approach isn't perfect, but it's an example of a corporate citizen taking up the cyber longbow on its own.

---

[70] "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or force citizens to confess by word or act their faith therein" *West Virginia v. Barnette*, 319 U.S. 624, 625 (1943).

[71] Matthew Weybrecht, *Free Speech in an Era of Self-Radicalization*, LAWFARE (Feb. 26, 2016), https://www.lawfareblog.com/free-speech-era-self-radicalization.

[72] *Microsoft's Approach to Terrorist Content Online* (May 20, 2016), https://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000g8l17to0xdtzrca20pluw755v.

The involvement of private entities in national cyber security is particularly important because they can act in ways the government cannot, and act with information they already have in the course of business or from open sources. Many government activities would require accessing online information, yet proposals that make it easier – or even appear to make it easier – for the government to access private information are instantly condemned.[73] The 2013 revelations of Edward Snowden caused a firestorm of protests against the NSA's surveillance activities, even though the spying programs were lawful under U.S law. The passing of the Cyber Intelligence Sharing and Protection Act (CISPA)[74] in 2013 and Protecting Cyber Networks Act (PCNA)[75] in 2015 also caused public outrage.[76] There simply seems to be a consensus, at least among politically active citizens, that the government should not be allowed to access and monitor large quantities of citizens' data, even to better ensure the security of the U.S.[77]

---

[73] Sorcher, *Digital activists begin broad, grass-roots battle to fight anti-encryption bill*, PASSCODE (Apr. 15, 2016), http://www.csmonitor.com/World/Passcode/2016/0415/Digital-activists-begin-broad-grass-roots-battle-to-fight-antiencryption-bill?cmpid=ema:nws:Daily%2520Newsletter%2520%2804-15-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160415_Newsletter:%20Daily&utm_term=Daily.

[74] CISPA directs the federal government to conduct cybersecurity activities to provide shared situational awareness enabling integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents. https://www.congress.gov/bill/113th-congress/house-bill/624.

[75] This amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal governmental agencies, or state, tribal, or local governments; and (2) the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts. https://www.congress.gov/bill/114th-congress/house-bill/1560.

[76] https://static.newamerica.org/attachments/2885-coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-pcna/Coaltion%20Letter%20Strongly%20Opposing%20PCNA.b24d1869025848cb96385603d8208dea.pdf.

[77] Deena Zaru, *Dilemmas of the Internet age: privacy vs. security*, CNN (Mar. 29, 2014), http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/.

Even the FBI's request for Apple to crack the encryption on the iPhone belonging to the San Bernardino shooter has generated outrage in a large segment of the population.[78] U.S. citizens have an increasing fear of governmental violations of privacy. A majority of the American people don't trust the government, and are concerned that the government's access to private information will result in violations of privacy and free speech.[79]

From the FBI's perspective, this was an easy call. The phone's owner was dead, along with the privacy interests, and his phone may have contained information to help stop other terrorist attacks. Although Apple didn't have the ability to crack the phone's encryption, it seemed the corporation would be best positioned to develop the capability to assist in the case.[80] The privacy community (and Apple) saw it differently, however.

Apple asserted that developing the technique would set a dangerous precedent and would create a threat to the data security of its customers.[81] In the end, Apple refused to budge and the FBI contracted with an information security company that was able break the encryption on the phone so the FBI could access the information.[82]

---

[78] Kim Zetter, *Apple's FBI Battle Is Complicated. Here's What's Really Going On*, WIRED (Feb. 18, 2016), https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/.

[79] A recent study conducted by Pew Research Center found that only 19% of Americans trust the government. Henry Gass, *How do Americans view government? Survey finds both distrust and hope*, CHRISTIAN SCI. MONITOR (Nov. 23, 2015), http://www.csmonitor.com/USA/Politics/2015/1123/How-do-Americans-view-government-Survey-finds-both-distrust-and-hope.

[80] *See* Zetter, *Apples FBI Battle is Complicated. Here's What's Really Going on*, WIRED (Feb. 18, 2016), https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/.

[81] Tim Cook, *A Message to Our Customers* (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[82] Julia Edwards, *FBI paid more than $1.3 million to break into San Bernardino iPhone*, REUTERS (Apr. 22, 2016), http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB. After the FBI reported it had accessed the phone, Apple demanded that the FBI tell it about the vulnerability used so the weakness could be patched. Conner Forrest, *Apple demands to know how FBI cracked*

Constitutional protections have given U.S. citizens the freedom to take risks and be creative, and the ability to push back against government programs that implicate privacy or personal property. This arrangement greatly facilitated the success of the U.S. economy and, as a result, U.S. international relations. Of course, the irony in the situation is that the very freedoms that facilitated the U.S. rise to superpower status in the physical world now impair U.S. efforts to be similarly dominant in cyberspace. By contrast, cyberspace has given U.S. rival States and groups another chance to be dominant, and some of them are seizing it with both hands. The lack of freedom may have limited rival States' innovation and progress previously, but the same set of circumstances allow their leadership to push forward in cyberspace, unconstrained by concerns over privacy and other constitutional rights. There must be a middle ground that would permit U.S. activities in the area to advance national security and still provide appropriate protections, even if not absolute dominance, for citizens' privacy.

VI. CONCLUSION

Cyberspace is constantly shifting as new nodes are added and others disappear. Locations of interest move (a network address can change) and are concealed (a network address can be spoofed) with ease. National security laws and strategy were conceived with physical boundaries in mind, but national borders in cyberspace are porous and uncertain.[83] These factors increase the complexity of cyber operations. Defining cyberspace more accurately as two separate elements, infrastructure and content, may help to refocus U.S. strategy going forward.

San Bernardino iPhone, TECH REPUBLIC (Mar. 30, 2016), http://www.techrepublic.com/article/apple-demands-to-know-how-fbi-cracked-san-bernardino-iphone/.When and if the government has an obligation to disclose vulnerabilities is another fascinating debate that is beyond the scope of this article.

[83] Miller, Brickey & Conti, *Why Your Intuition about Cyber Warfare is Probably Wrong*, SMALL WARS JOURNAL (Nov. 29, 2012), http://smallwarsjournal.com/print/13573.

The success of others in the ideosphere, particularly Russia and ISIS, is frustrating, because it is precisely the type of thing Americans are typically good at. Generally, the U.S. does well in the ideosphere (freedom, culture, etc.), but is not as successful as other actors in driving towards specific goals. If the U.S. hopes to operate more successfully in cyberspace it needs to look at things differently. There will be occasions where engaging on cyber infrastructure will be the best tactic, certainly when it is in conjunction with armed conflict. In other cases, maximum effectiveness will be found in taking on the adversary in the ideosphere. Examples may include debating issues, undercutting positive adversary information, manipulating information and the trust placed in it, and preventing the efficient flow of that information.[84]

England's dominance in 14th century military affairs wasn't due to a secret weapon that no one else could obtain. Rather, England's military reigned supreme in the era because its adversaries feared empowering the public to fully participate in national security. The dominance endured until England's rivals decided the rewards of extending capability beyond the elites to the population outweighed the risks. America's adversaries have successfully weaponized social media.[85] How long will it be before the U.S. unleashes its own cyber longbow, employing non-traditional assets for the on-going clashes in cyberspace?

Rather than remaining merely another of the "weary giants of flesh and steel," there is a need for the U.S. to engage in "the new home of Mind."[86] U.S. leadership in cyberspace is vital to ensure it remains a powerful, albeit flawed, force for progress and creation.

---

[84] Maybe sending comedians to engage with ISIS, as the band U-2's Bono suggests, would help solve the problem. Or maybe not. *Bono: send Amy Schumer and Chris Rock to fight Islamic State*, THE GUARDIAN (Apr. 13, 2016), https://www.theguardian.com/music/2016/apr/13/bono-send-amy-schumer-chris-rock-fight-islamic-state-isis.

[85] Emerson T. Brooking & Peter W. Singer, *War Goes Viral*, THE ATLANTIC (Nov. 2016), http://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

[86] John Perry Barlowe, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FREEDOM FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

Competing will require employing citizens in the protection of the nation, primarily addressing the information that represents human interaction and all the inherent risks and rewards, with the physical components of the internet playing a supporting role.