NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
15 N.C. J.L. & TECH. ON. 134 (2014)

COUNTERATTACKING THE COMMENT CREW: THE CONSTITUTIONALITY OF PRESIDENTIAL POLICY DIRECTIVE 20 AS A DEFENSE TO CYBERATTACKS

Nicholas Ryan Turza*

Presidential Policy Directive 20 authorizes the United States government to counterattack state-sponsored hackers who target America from overseas, such as recent malefactors from Syria and China. However, despite actively legislating in the field of cybersecurity, no act of Congress authorizes or rejects Presidential Policy Directive 20. Because an execution of the directive could cause collateral damage to domestic computer networks, the Supreme Court's balance-of-powers precedents, such as Youngstown Sheet & Tube Co. v. Sawyer *and* United States v. Curtiss-Wright Export Corp.*, question the constitutionality of any cyberattack the President orders as domestic, rather than foreign policy.*

I. INTRODUCTION

Cyberattacks threaten America's national security.[1] Congress has instituted criminal and civil penalties for criminal hacking, but

* J.D. Candidate, University of North Carolina School of Law, Class of 2015; M.P.P. Candidate, Sanford School of Public Policy, Duke University, Class of 2015. Author separated as a Captain in the Army after eight years of service, with combat tours in Iraq and Afghanistan. The author appreciates the work of the editors who helped him through multiple drafts and hurdles, particularly Laura Arredondo-Santisteban, Virginia Wooten, Cara Richards, and Kaitlin Powers.

[1] *See* Derek S. Reveron, *An Introduction to National Security and Cyberspace*, *in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD 3, 9 (Derek S. Reveron ed., 2012) [hereinafter CYBERSPACE AND NATIONAL SECURITY] (discussing a milieu of strategies issued by the Department of Defense to address the increasing threat in cyberspace, and referencing a former NATO commander's declaration that "[t]he cybersecurity threat is real [because] [a]dversaries target networks, application software, operating systems, and even the ubiquitous silicon chips inside computers, which are the bedrock of [U.S. infrastructure]").

America is increasingly in the crosshairs of overseas cyberattacks supported by foreign governments. Accordingly, in October 2012, President Obama signed Presidential Policy Directive 20 ("PPD20"),[2] a "Top Secret / No Foreign"[3] executive order directing the federal government to act defensively in cyberspace and, if necessary, counterattack with offensive cyber operations.[4] PPD20 directs the United States Government ("USG") to ready a list of foreign targets for the United States to strike with a cyberattack if so ordered by the President,[5] and issues guidance for emergency actions that a department could trigger with the President's approval.[6] The document concedes that operations directed under its framework may lead to "cyber effects," a vague term used throughout the order,[7] in "locations other than the intended target,

[2] Presidential Policy Directive 20, U.S. CYBER OPERATIONS POLICY, 9 (Oct. 16, 2012), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf [hereinafter PPD20].

[3] Despite its classification, the British press attained a leaked copy and published it in the summer of 2013. *See* Glenn Greenwald & Ewen MacAskill, *Obama Orders Us to Draw up Overseas Target List for Cyber-Attacks*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[4] PPD20 first defines the operations it authorizes before authorizing those operations. *See* PPD20, *supra* note 2, at 3, 4 (stating the government "shall conduct all cyber operations" when discussing the purpose of scope of the order)*; see also* Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, WASH. POST (Nov. 14, 2012), http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

[5] *See* PPD20, *supra* note 2, at 9 ("The United States Government shall identify potential targets of national importance where OCEO [Offensive Cyber Effects Operations] can offer a favorable balance of effectiveness and risk as compared with other instruments of national power . . . and execute those capabilities in a manner consistent with the provisions of this directive.").

[6] *See id.* at 3–4 (defining the scope and conditions of an "Emergency Cyber Action").

[7] *Id.* at 9. The Directive does not specify what cyber effects are or give examples, but an assessment of what types of actions would cause them are found *infra* Part IV.B.

with potential unintended or collateral consequences that may affect U.S. national interests in many locations."[8]

Beyond any policy debate of how aggressive the USG should be in addressing cyberattacks, the President's unilateral action through PPD20 raises constitutional questions of the proper balance of powers between the government's legislative and executive branches. While the President is the Commander-in-Chief, that grant of authority in Article II of the Constitution does not leave the President with unchecked power for all matters related to national defense.

This Recent Development asserts that the constitutionality of an executive order directing those steps is questionable because Congress, which the Constitution also assigns a role in safeguarding America's national defense and regulating the interstate commerce that is conducted over America's computer networks, has passed civil and criminal statutes to govern cybersecurity. Congress has not, however, specifically deliberated (at least publically) upon the provisions of PPD20, let alone endorsed the measures it authorizes. Because the Supreme Court's precedent regarding the balance of powers in national security has cemented a role for Congress,[9] this Recent Development argues the President's actions in executing PPD20 without Congress's approval might only be deemed constitutional if the President can prove the action fits into a category of general deference the Court has often—but not always—afforded the President in matters of foreign, as opposed to domestic, affairs.

Part II of this Recent Development provides an overview of the national security threat posed by foreign hackers. Part III discusses how Congress has governed the field of cybersecurity but has not passed legislation sufficient to protect the United States from foreign cyberattacks. Part IV describes PPD20. Part V analyzes PPD20 under governing Supreme Court decisions, and Part VI applies this legal framework to two hypotheticals, one involving foreign action and one involving domestic action.

---

[8] PPD20, *supra* note 2, at 6.
[9] *See infra* Part V.A.

II. THE DANGER OF FOREIGN CYBER THREATS TO NATIONAL SECURITY

The infrastructure of the Internet is as vulnerable as it is critical.[10] Cybercrime and internet-based corporate espionage have become everyday realities of the information age.[11] Although the public has not historically placed much emphasis on cybercrimes because their total costs are relatively minor compared to the global economy,[12] the dangers of cyber warfare are becoming increasingly apparent as governments have used hacking to target opposition, steal secrets, and wage war. The number of strategic cyberattacks from foreign governments is increasing as some countries aim to use the Internet to launch geopolitical assaults on the United States.[13] Cyberwarfare expert James Lewis testified to

---

[10] *Cybersecurity: Assessing the Immediate Threat to the United States: Hearing Before the Subcomm. on Nat'l Sec., Homeland Def. and Foreign Operations of the H. Comm. on Oversight and Gov't Reform*, 112th Cong. 26 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg70676/pdf/CHRG-112hhrg70676.pdf (prepared statement of James A. Lewis, Director, Technology and Public Policy Program, Center for Strategic and International Studies) [hereinafter *Cybersecurity*].

[11] For a background on the spread of cybercrime, to include intellectual property theft, throughout the criminal world in general, see generally KRISTIN M. FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT (2013):

> [C]riminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking. In addition, they exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft. The Federal Bureau of Investigation (FBI) considers high-tech crimes to be the most significant crimes confronting the United States.

Id.

[12] *The Economic Impact of Cybercrime and Cyber Espionage*, CSIS & MCAFEE 3 (July 2013), *available at* http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf (explaining that, even with liberal cost estimates, the losses are only "a fraction of a percent of global income").

[13] *See* Brandon Valeriano & Ryan Maness, *Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare*, *in* CYBERSPACE AND NATIONAL SECURITY 139, 144 (Derek Reveron ed., 2012) (analyzing cyberwarfare and interstate rivalry).

Congress that "the greatest threats come from advanced, state-sponsored actors who have the skill and resources to overcome most defenses."[14] Two current threats, one from Syria and one from China, are emblematic of this national security threat from hackers overseas, while the Russian use of hacking in their international conflicts shows the level of danger that could be on the horizon from a new weapon of war.

A. *Syria and the Proliferation of Arms*

The Syrian Electronic Army ("SEA") is illustrative of how America's "minor" international adversaries are attaining the power—and willpower—to conduct cyberattacks against the United States. In contrast to their evaluations of China, Russia, and Iran, national security experts did not consider Syria to be a cyberwarfare "heavyweight" in a 2010 global assessment.[15] The SEA emerged to oppose the 2011 anti-Assad revolt as a hierarchal organization of hackers, media supporters, and pro-Assad volunteers.[16] SEA members claim they support Assad independently, but significant evidence links SEA attacks to the regime,[17] and the organization is historically rooted in a group Assad led before ascending to the presidency.[18]

---

[14] *Cybersecurity*, *supra* note 10, at 5.

[15] Other nations in the "heavyweight" category are the United States, the United Kingdom, Israel, France, Germany, India, Pakistan, Belarus, and Ukraine. *See* Valeriano & Maness, *supra* note 13, at 145 (discussing RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010)).

[16] Nicole Perlroth, *Hunting for Syrian Hackers' Chain of Command*, N.Y. TIMES (May 17, 2013), http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=0.

[17] The evidence includes tracing the attacks to servers owned by Assad's cousin and the conduct of SEA actions against Syrian opposition figures. *See id.*

[18] *See id.* (recounting how the SEA grew out of a "technical organization" led by Assad).

On August 27, 2013, the SEA shut down the *New York Times*.[19] Although the newspaper has long proclaimed it publishes "All the News That's Fit to Print,"[20] the newspaper's greatest reach is online.[21] SEA hacking blocked access to nytimes.com after the site substantiated United States claims that Syria used sarin gas on its own people.[22] This "Domain Name System (DNS) hijacking" occurred just as President Obama sought domestic and international support to militarily deter Syria's chemical weapon use.[23] The *New York Times* attack may have become the SEA's most infamous cyberattack on a major media outlet, but it was not its only one.[24] In the eyes of the SEA, the targets—various media organizations—had posted articles with undue sympathy for Syrian

[19] *"Syrian Electronic Army" Takes Credit For Hacking New York Times Website*, CBS NEWS (Aug. 27, 2013), http://www.cbsnews.com/8301-201_162-57600369/syrian-electronic-army-takes-credit-for-hacking-new-york-times-website/.

[20] The *New York Times* has printed the slogan on Page 1 since 1897. *Who We Are*, THE NEW YORK TIMES COMPANY, http://www.nytco.com/who-we-are/culture/our-history/ (last visited Oct. 30, 2013, 12:22 PM).

[21] The newspaper's website, nytimes.com, reaches nearly 30 million individuals every month. *See* Russell Adams, *New York Times Readies Pay Wall*, WALL ST. J. (Jan. 24, 2011), http://online.wsj.com/article /SB10001424052748704213404576100033883758352.html; *see also May 2012 – Top U.S. Web Brands and News Websites*, NIELSON (June 22, 2012), http://www.nielsen.com/us/en/newswire/2012/may-2012-top-u-s-web-brands-and-news-websites.html.

[22] *See* Ben Hubbard, Mark Mazzetti & Mark Landler, *Blasts in the Night, a Smell, and a Flood of Syrian Victims*, N.Y. TIMES (Aug. 26, 2013), http://www.nytimes.com/2013/08/27/world/middleeast/blasts-in-the-night-a-smell-and-a-flood-of-syrian-victims.html (substantiating U.S. claims about the gas attack).

[23] The headline of an indicative article posted online by the *Times* at the time of the attack was, "Not Easy to Hide a Chemical Attack, Experts Say." *"Syrian Electronic Army" Takes Credit For Hacking New York Times Website*, *supra* note 19.

[24] *See id.* ("The [SEA] has, in recent months, taken credit for Web attacks on media targets . . . including prior attacks at the New York Times, along with the Washington Post, Agence France-Presse, 60 Minutes, CBS News, National Public Radio, The Associated Press, Al-Jazeera English and the BBC.").

rebels or unjust prejudice against President Assad and the Syrian military.[25]

The simplicity of the SEA's Internet hijacking masks both the danger it poses and its growing ambitions.[26] In April of 2013, the SEA hijacked the Associated Press Twitter account and tweeted a fake news story about a terrorist attack on the White House, causing a $136 billion stock market loss in response to the fake story.[27] The SEA has also employed simple cyber-hijacking techniques to spy on, geographically locate, and publically pinpoint Syrian rebels.[28] And while the degree to which the SEA's threatened cyberattacks contributed to the reluctance to support President Obama's proposed strikes is unknown, the counterattack factored into the national conversation.[29] American intelligence agencies briefed the cyberattack risk to Congress as they considered the President's request to launch a military strike, and

---

[25] *See id.* (discussing the SEA's motives).

[26] *See* Shane Harris, *How Did Syria's Hacker Army Suddenly Get so Good?*, FOREIGN POL'Y (Sept. 3, 2013, 8:10 PM), http://killerapps.foreignpolicy.com/posts/2013/09/03/how_did_syrias_hacker_army_suddenly_get_so_good ("As the SEA's ambition has grown, so has its skill level. The attack on the New York Times effectively gave the group control of the entire Web site. It was accomplished not by a frontal assault, but by changing information in the Domain Name System databases via a company in Australia. Anyone who tried to visit the Times Web site was redirected to another site under the SEA's control, sporting its logo. Not exactly high-end tradecraft, but not the work of simple vandals, either, which is what the SEA has long been known for.").

[27] *See* Veronica Bautista, *You've Been Hacked by the Syrian Electronic Army*, ABC NEWS (Sept. 4, 2013), http://fusion.net/abc_univision/story/youve-hacked-syrian-electronic-army-10407; *see also* Peter Foster, *'Bogus' AP Tweet About Explosion at the White House Wipes Billions off US Markets*, THE TELEGRAPH (Apr. 23, 2013), www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

[28] *See* Harris, *supra* note 26.

[29] *See* Paul Steinhauser & John Helton, *CNN Poll: Public Against Syria Strike Resolution*, CNN.COM (Sept. 9, 2013, 12:49 PM), http://www.cnn.com/2013/09/09/politics/syria-poll-main/ ("Fifty-nine percent of people questioned say they don't think Congress should approve a proposed resolution authorizing military action against Syria for up to 90 days—an initial 60-day window plus another 30 following congressional notification—but prohibiting the use of ground troops. About 40% support that plan.").

the media reported how the FBI was warning blue chip companies to gird themselves for a wave of cyberattacks if the President pulled the trigger against Assad.[30]

B. *China and the Comment Crew*

If the Syrian Electronic Army represents the growing threat from minor adversaries and "rogue states," the Comment Crew symbolizes a threat to America from a major adversary. The Chinese People's Liberation Army ("PLA") not only constitutes the world's largest military force,[31] but it also boasts a sophisticated corps of hackers, operating out of a single twelve-story building in the Pudong district of Shanghai.[32] PLA Unit 61398, known internationally as the Comment Crew or APT1,[33] "has drained terabytes of data" from scores of American international firms, and "increasingly its focus is on companies involved in the critical infrastructure of the United States—its electrical power grid, gas lines, and waterworks."[34]

As with the SEA, digital forensic evidence links the hackers to the supportive government.[35] Comment Crew hackers are far more capable than the SEA by virtue of a strong institutional and physical infrastructure to support their operations.[36] In a comprehensive report on Unit 61398, the security firm Mandiant

---

[30] *See* Harris, *supra* note 26.

[31] *China's Military Rise: The Dragon's New Teeth*, THE ECONOMIST (Apr. 7, 2012), http://www.economist.com /node/21552193 ("The PLA is still the largest army in the world, with an active force of 2.3m[illion].").

[32] *See* David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html? (tracing the evidence back to the unit's operational hub in Shanghai and discussing its operations).

[33] Charlie Osborne, *Chinese Military Linked to 'Overwhelming' Number of Cyberattacks*, ZDNET (Feb. 19, 2013, 12:17 AM), http://www.zdnet.com/chinese-military-linked-to-overwhelming-number-of-cyberattacks-7000011484/.

[34] *See* Sanger, Barboza & Perlroth, *supra* note 32.

[35] *See* Osborne, *supra* note 33 (explaining how computer experts trace the attacks back to Shanghai).

[36] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 4–5 (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

identified 141 successful infiltrations of companies, sometimes conducted simultaneously, over a period of hacking stretching back to 2006.[37] The report concluded that "all industries related to *China's strategic priorities* are potential targets of [Unit 61398]'s comprehensive cyber espionage campaign."[38] This conclusion highlights the difference between these attacks and routine corporate espionage: Beijing is stealing information for the strategic purpose of challenging American power globally.[39]

The threat from Unit 61398 is growing beyond theft of technological advancements and trade secrets. For example, cybersecurity researcher Kyle Wilhoit used a "honeypot"—a dummy control system serving as a virtual decoy—to study if criminal hackers, usually out for profit, would go so far in their hacking as to attempt to compromise a water control system for a U.S. municipality.[40] Wilhoit instead caught the Comment Crew hacking into his decoy, attempting to gain a level of access sufficient to control the water utility.[41]

---

[37] *Id.* at 3.

[38] *Id.* at 24 (emphasis added).

[39] Further supporting that notion is the evidence of targeting of military technology by Chinese hackers. *See 'Little or No Warning': Obama Draws up Worldwide Cyber-Attack Target List*, RT.COM (Jun. 11, 2013, 8:59 AM), http://rt.com/usa/obama-cyber-attack-list-418/ ("[Secretary of Defense] Hagel's comments [about Chinese hacking] came in the wake of a . . . report which claimed around 40 Pentagon weapons programs and almost 30 other defense technologies had been compromised by Chinese hackers, some purportedly tied to the military or government.").

[40] Tom Simonite, *Chinese Hacking Team Caught Taking over Decoy Water Plant*, MIT TECH. REV. (Aug. 2, 2013), http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/. This technique was technically a SCADA honeypot, a honeypot specifically "used to lure industrial hackers." *See MIT Says that Honeypots Can Lure Industrial Hackers into the Open*, IT SECURITY PRO (July 10, 2013), http://itsecuritypro.co.uk/morestories/mit-says-that-honeypots-can-lure-industrial-hackers-into-the-open/.

[41] *Id.* Wilhoit recorded seventy-four attacks from sixteen different countries; half of the critical attacks came from China. *Id.* (" 'You would think that Comment Crew wouldn't come after a local water authority,' Wilhoit [said], but the group clearly didn't attack the honeypot by accident while seeking another

C. *Russian Zombies and the Future of Threats*

Distributed denial of service ("DDoS") attacks constitute the carpet bombing of the digital battlefield.[42] Although originally used by "criminals and non-state actors,"[43] these attacks have increasingly occurred in international conflicts between nation-states.[44] A DDoS attack will deny service to a target network through "a coordinated effort that instructs [personal computers] to send a victim a flood of traffic designed to overwhelm [the victim's] servers or consume their bandwidth."[45] DDoS hackers "distribute" their attacks by engaging "thousands, even hundreds of thousands of computers . . . called a 'botnet,' a robotic network of 'zombies,' computers that are under remote control."[46] Owners of zombie computers usually have little to no clue a hacker is controlling their computers for a DDoS attack: "The malicious activity is all taking place in the background, not appearing on the user's screen. Your computer, right now, might be part of a botnet."[47]

Pro-Russian hackers[48] have twice launched significant DDoS attacks against former Soviet states when those former satellites

---

target. 'I actually watched the attacker interface with the machine,' says Wilhoit. 'It was 100 percent clear they knew what they were doing.' ").

[42] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED.COM (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/ 15-09/ff_estonia?; *see also* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 284 (2010) (defining DDoS as a "basic cyber war technique").

[43] *See* CLARKE & KNAKE, *supra* note 42, at 284.

[44] *See* Jose Nazario, *Politically Motivated Denial of Service Attacks*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 163 (Christian Czosseck and Kenneth Geers, eds. 2009) (examining how DDoS attacks, even if seemingly guided by non-state actors, played a significant role in sixteen specific instances of intra and international conflict).

[45] *Id.*

[46] *See* CLARKE & KNAKE, *supra* note 42, at 14.

[47] *Id.*

[48] No expert has ever been able conclusively attribute the activity back to President Putin's government itself, which always denies direct involvement, but the suspicion exists. In regard to the Estonia attack, see CLARKE & KNAKE, *supra* note 42, at 15–16 ("The Russian government indignantly denied that it was engaged in cyber war against Estonia. . . . Informed that the attacks had

challenged Moscow's hegemony. After a flare-up of historical tensions, these hackers first attacked Estonia, "the most wired country in Europe,"[49] with a DDoS of an unprecedented scale.[50] Millions of zombie computers ("zombies") shut down the Internet capabilities of Estonia's largest bank, Estonia's government sites, the communication between government offices, and Estonia's media outlet's access to their readers.[51] Although the attacks eventually abated, Estonia felt so threatened that the new NATO member raised its concerns with the highest council of the alliance for discussion.[52]

In a similar DDoS event, Russian hackers used the same technique to block Georgia's international banking during the Russian-Georgian war of 2008.[53] Although the DDoS attack was a minor concern relative to the physical invasion by Russian troops,[54] the degree of coordination of the virtual attack of a country's

---

been traced back to Russia, some government officials admitted that it was possible perhaps that patriotic Russians, incensed at what Estonia had done, were taking matters into their own hands. Perhaps.") In regard to the Georgia attack, see CLARKE & KNAKE, *supra* note 42, at 20 ("As in the Estonian incident, the Russian government claimed that the cyber attacks were a populist response that was beyond the control of the Kremlin. A group of Western computer scientists, however, concluded that the websites used to launch the attacks were linked to the Russian intelligence apparatus.").

[49] *See* Davis, *supra* note 42.

[50] The removal of Soviet statue by the Estonian government lit a powder keg of decades-old tensions between ethnic Estonians and Russian Estonians, leading to riots between the two groups in Tallinn streets and "indignant nationalist responses" by Russians in Moscow in the spring of 2007. *See* CLARKE & KNAKE, *supra* note 42, at 13.

[51] *See* CLARKE & KNAKE, *supra* note 42, at 13.

[52] *See* Davis, *supra* note 42 (reporting how Estonia's parliament speaker believed the attack was checking NATO's defenses); *see also* CLARKE & KNAKE, *supra* note 42, at 15 (narrating Estonia's domestic and international response steps).

[53] *See* CLARKE & KNAKE, *supra* note 42, at 17–21 (describing the coordinated and adaptive DDoS attack on Georgia).

[54] Aaron Mannes & James Hendler, *The First Modern Cyberwar?*, THE GUARDIAN (Aug. 22, 2008), http://www.theguardian.com/commentisfree/2008/aug/22/russia.georgia1 (concluding the DDoS attacks were a "sideshow" in comparison to the ground invasion of Georgia by the Russian military).

network with the physical invasion of territory was unprecedented.[55] Russia's coordination intentionally avoided targeting critical infrastructure that could cause chaos or interfere with Western nations' interests, particularly oil pipelines; however, the Russians' actions signaled that they had that capability.[56]

III. CONGRESSIONAL CYBERSECURITY LEGISLATION

The Computer Fraud and Abuse Act ("CFAA")[57] and the Economic Espionage Act of 1996 ("EEA")[58] criminalize hacking, so the SEA's routine hacking and DDoS attacks violate the CFAA,[59] and Unit 61398's espionage *would* violate the EEA if the offenders were Americans or were in the United States.[60] As the centerpiece of cybersecurity law, the aggressive CFAA not only criminalizes the hacking of any American computer connected to the Internet, but it is so broadly worded that it could make a federal case out of routine web surfing in the workplace.[61] The EEA

---

[55] David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J. 2 (2011), *available at* http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 ("This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space).").

[56] *Id.* at 4 (quoting John Bumgarner of the U.S. Cyber Consequences Unit: "For example, [the Russian hackers] didn't attempt to cripple sites that could have caused chaos or injury, such as those linked to power stations or oil-delivery facilities . . . There was a political decision not to attack those critical infrastructures directly. They made the point that they could launch these attacks. They showed they have the capability to do more[.]").

[57] 18 U.S.C. § 1030 (2012).

[58] 18 U.S.C. § 1831 (2012).

[59] *See* Charlotte Decker, Note, *Cyber Crime 2.0: An Argument To Update The United States Criminal Code To Reflect The Changing Nature Of Cyber Crime*, 81 S. CAL. L. REV. 959, 978–85 (2008) (explaining the application of the CFAA to general intrusions and damages to content and referencing a federal guilty plea in a CFAA charge against a DDoS hacker who targeted eBay).

[60] *See* 18 U.S.C. § 1837 (2012) (stating the EEA "also applies to conduct occurring outside the United States" but only if the offenders are U.S. citizens or permanent residents or if "an act in furtherance of the offense was committed in the United States").

[61] *See* Paul Larkin, *Reasonably Construing the Computer Fraud and Abuse Act to Avoid Overcriminalization*, THE HERITAGE FOUNDATION (June 19, 2013), http://www.heritage.org/research/reports/2013/06/reasonably-construing-the-

protects American commerce and industry against corporate espionage conducted through the Internet, and specifically enables U.S. Attorneys to prosecute a hacker for the eponymous crime.[62] However, for reasons discussed below, both laws are ineffective against a hacker working from abroad and supported by a foreign government.

A. *Computer Fraud and Abuse Act*

The CFAA, nearly 30 years old, has become "the king of all computer fraud laws."[63] Prosecutors use it frequently,[64] Congress has updated it regularly,[65] and it includes both civil and criminal provisions.[66] While the CFAA's roots arguably lie in national security concerns,[67] the CFAA is now used not only for domestic prosecution but also litigation.[68]

---

computer-fraud-and-abuse-act-to-avoid-overcriminalization ("The broad interpretation [of the CFAA] protects against the misuse of lawfully obtained information, but it also would make it a crime for an employee to use his work computer to access the Internet in order to check his standing in a fantasy football league or for any of the myriad other harmless reasons why a person would surf the net.").

[62] 18 U.S.C. § 1831 (2012).

[63] Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"- A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 154 (2011).

[64] *Id.* at 154 ("The [CFAA] is the most frequently used law for combating computer fraud."); *see also* Grant McCool, *Computer Fraud and Abuse Act: The 1980s-Era Hacking Law Out Of Step With Today's Internet, Analysts Say*, THE HUFFINGTON POST (Jul. 29, 2012, 10:43 AM), http://www.huffingtonpost.com/2012/07/29/computer-fraud-and-abuse-act_n_1716058.html ("Prosecutors have brought about 550 federal criminal cases under the CFAA and related computer fraud laws in the past 5-1/2 years. . . .").

[65] *See* Tuma, *supra* note 63, at 156 ("The CFAA has been amended frequently to enable it to keep abreast with technological advances.") (citing Deborah F. Buckman, *Annotation, Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. FED. 101 (2001)).

[66] *See id.* at 155 ("Initially a federal criminal statute, the CFAA was subsequently expanded to permit the recovery of civil damages and injunctive relief for certain of its violations.").

[67] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010) ("The first offenses protected classified national security secrets. . . . All three statutes were tailored to a

Accordingly, the CFAA debate today centers around domestic applications. Critics from across the political spectrum have voiced frustration with the prosecutions executed by U.S. Attorneys through the open-ended language of the statute.[69] The Ninth Circuit has echoed critics' concerns of the CFAA's excessive breadth,[70] but the Department of Justice ("DoJ") recommends making the law even tougher.[71] As Congress is considering a bill with the changes urged by the DoJ,[72] the debate shows congressional willingness to govern the field of cybersecurity. However, the debate also shows Congress is legislating in a way that focuses on domestic issues and ignores the

---

specific government interest: national security, financial records, and government property.") (citing 18 U.S.C. § 1030(a)(1)–(3) (1985)*; see also* Ellen S. Pogdor, *Computer Crimes and the USA PATRIOT Act*, 17 CRIM. JUST. 61 (2002), *available at* http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust _cjmag_17_2_crimes.html (discussing changes made throughout 18 U.S.C. § 1030 by § 814 of the Patriot Act).

[68] *See* Tuma, *supra* note 63, at 154; *see also* McCool, *supra* note 64 (stating that in a recent five-and-a-half year span "nearly 500 civil lawsuits were brought in private disputes citing the CFAA and related laws").

[69] *See* Ryan J. Reilly, *Zoe Lofgren Introduces 'Aaron's Law' To Honor Swartz On Redditt*, THE HUFFINGTON POST (Jan. 15, 2013, 11:24 PM), http://www.huffingtonpost.com/2013/01/15/zoe-lofgren-aarons-law-swartz_n_2483770.html; *see also* Larkin, *supra* note 61.

[70] United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty."); *see also* McCool, *supra* note 64 (discussing how the *Nosal* holding could lead to adjudication by the U.S. Supreme Court).

[71] *See* Orin Kerr, *House Judiciary Committee New Draft Bill on Cybersecurity is Mostly DOJ's Proposed Language from 2011*, VOLOKH CONSPIRACY (Mar. 25, 2013, 5:30 PM), http://www.volokh.com/2013/03/25/house-judiciary-committee-new-draft-bill-on-cybersecurity-is-mostly-dojs-proposed-language-from-2011/ (discussing, and criticizing, the DoJ language that Senators and House Representatives have adopted in their bill drafting).

[72] *See* Paul Rosenzweig, *House Judiciary CFAA Bill*, LAWFARE (Mar. 26, 2013, 2:19 PM), http://www.lawfareblog.com/2013/03/house-judiciary-cfaa-bill/ (noting the bill "seems to answer most of what the Department of Justice wants with very little for the internet online community in return"). *See generally* Peter Toren, *Amending the Computer Fraud and Abuse Act*, 14 COMPUTER TECH. L. REP. (BNA) 8, Apr. 19, 2013, at 256 (discussing the debate in Congress).

threat from foreign nations. No matter how broad the law's scope, with traditional criminal and civil provisions and penalties it cannot encompass threats such as the Chinese military. An FBI agent cannot fly into Shanghai and handcuff a Chinese soldier for violating American criminal law, particularly when his military mission is to do so.[73] If Congress endeavors to tackle the foreign threat, Congress should consider authorizing other strategies. One such strategy is PPD20, but Congress has not deliberated on PPD20's tactics.

B. *Economic Espionage Act of 1996*

Congress passed the EEA in 1996 to enable Federal prosecutors to address theft of proprietary information such as trade secrets.[74] The EEA criminalizes all such theft, including theft that occurs over the Internet.[75] The EEA has two separate offenses, one for general theft of trade secrets in the course of interstate commerce,[76] and another, § 1831, for economic espionage intended to benefit a foreign power,[77] under which U.S. Attorneys rarely

[73] *See generally* Mark M. Jaycox, *Increasing CFAA Penalties Won't Deter Foreign "Cybersecurity" Threats*, ELECTRONIC FRONTIERS FOUNDATION DEEPLINKS BLOG (Apr. 11, 2013), https://www.eff.org/deeplinks/2013/04/increasing-cfaa-penalties-wont-deter-foreign-cybersecurity-threats (contrasting CFAA update proposals premised "as necessary to protect against foreign threats" with the reality that prosecutors will find it "hard, if not impossible" to extradite "state or quasi-state sponsored [hackers]" from such countries as China, Iran, or Russia).

[74] James Pooley, Mark Lemley & Peter Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 187 (1997).

[75] 18 U.S.C. § 1839(3) (2012) ("[T]he term 'trade secret' means *all forms and types of . . . information* . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, *electronically*, graphically, photographically, or in writing . . . .") (emphasis added); *see also* Ian C. Ballon, *Intellectual Property Law Update: The Internet Applications Of The Economic Espionage Act Of 1996*, 1 No. 11 CYBERSPACE LAW 13, Feb. 1997 ("The law also provides that a violation of the Economic Espionage Act of 1996 may be actionable under the Wire Tap Act, and therefore prohibits Internet interceptions (as well as theft). . . . [T]he Act is intended 'to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished.' ").

[76] 18 U.S.C. § 1832 (2012).

[77] 18 U.S.C. § 1831 (2012).

prosecute cases.[78] Although some commentators believe this under-prosecution originates from a lack of clarity in the law,[79] the fact that so many violations involve China[80] underscores a different reason prosecutions are rare: the violators are in China.

In January 2013, President Obama signed legislation to broaden the scope of espionage the EEA criminalizes and to increase the limit of penalties for violators.[81] However, neither amendment to the EEA deters state-sponsored hacking from overseas. Like the CFAA, the EEA's fundamental scope is limited: The EEA can only address hacking done by hackers that would be, in a practical sense, subject to the laws' provisions. Despite the law's intent to address the very espionage the Comment Crew conducts,[82] even the law's own language recognizes the outer limits of the law do not include foreign hackers operating overseas.[83]

---

[78] Recent Case, *Criminal Law – Economic Espionage – Ninth Circuit Upholds First Trial Conviction Under § 1831 of the Economic Espionage Act of 1996. –* United States v. Chung, *659 F.3d 815 (9th Cir. 2011),* cert. denied*, No. 11-1141*, *2012 WL 929750 (U.S. Apr. 16, 2012)*, 125 HARV. L. REV. 2177, 2177 n.3 (2012) (highlighting the difference between the 800 ongoing FBI investigations of economic espionage in 1996 and the small number, less than 60, of federal prosecutions of § 1831 cases twelve years later).

[79] *Id.* at 2182 ("EEA ambiguity disincentivizes prosecution of cases at the margin.").

[80] In the few § 1831 cases the government has prosecuted, "nearly all have involved China" in the sense that the origin of the espionage was either the Chinese government or a Chinese national. *See id.* at 2181–82.

[81] *See* Robert Milligan, *President Obama signs Economic Espionage Act amendments that significantly enhance the penalties for trade secret theft by foreigners*, LEXOLOGY (Jan. 15, 2013), http://www.lexology.com/library/detail.aspx?g=cd851e54-0793-4774-91e2-a9b9581746eb.

[82] *See* J. Thomas Coffin, *The Extraterritorial Application Of The Economic Espionage Act Of 1996*, 23 HASTINGS INT'L & COMP. L. REV. 527, 531 (2000) (recounting the EEA's legislative history: "the House made very clear its intent that a prime target of the EEA was the foreign agent who would appropriate trade secrets of an American company").

[83] *See* 18 U.S.C. § 1837 (2012).

IV. PRESIDENTIAL POLICY DIRECTIVE 20

Facing the rise of foreign-sponsored cyber threats with only the ineffective statutes of the CFAA and EEA, President Obama signed Presidential Policy Directive 20 in 2012.[84] The President addressed the top secret executive order to members of his National Security Council,[85] directing them to act assertively in cyberwarfare to guard against foreign threats.[86]

A. *Targeting, Effects, and the Rules of Engagement*

In contrast to the law enforcement statutes described above, PPD20 directs a military response to cyber threats. First, the directive requires the identification of "potential targets of national importance where [offensive cyber effects operations] can offer a favorable balance of effectiveness and risk as compared with other instruments of national power . . . ."[87] The press understandably focused on PPD20's authorization of a cyberattack "target list" in its reporting of the leak.[88]

Second, PPD20 authorizes offensive cyber effects operations ("OCEO") and defensive cyber effects operations ("DCEO").[89] The former "can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."[90] Both include "operations and related programs or activities [of the U.S.

---

[84] Nakashima, *supra* note 4.

[85] PPD20, *supra* note 2, at 1.

[86] *See* PPD20, *supra* note 2, at 4 ("The United States has an abiding interest in developing and maintaining use of cyberspace as an integral part of U.S. national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm U.S. national interests in peace, crisis, or war.").

[87] PPD20, *supra* note 2, at 9.

[88] As a prime example of how PPD20's target list attracted the most attention, see, e.g., Philip Bump, *Obama's Cyberwar Target List Just Made His Meeting with China Very Difficult*, THE ATLANTIC WIRE (June 7, 2013), http://www.theatlanticwire.com/politics/2013/06/obamas-cyberwar-target-list-china-xi/66022/.

[89] *See* PPD20, *supra* note 2, at 4 ("The United States Government shall conduct DCEO and OCEO . . . .")

[90] PPD20, *supra* note 2, at 9.

Government] in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks."[91]

Just as with the targeting terminology, PPD20's reliance on the term "effects," particularly to describe operations, highlights that PPD20 is, at its core, a military document. The concept of "Effects Based Operations" ("EBO") arose in American joint military doctrine during Desert Storm and the early 1990s as a "new way of war."[92] Although EBO died an early death when traditionalist generals secured its formal demise,[93] EBO was arguably ahead of its time. The Air Force, the branch that originally sponsored EBO, has resuscitated the doctrine in recent years.[94] A doctrine meant to advance airpower now fits cyberwarfare perfectly:

> The goal was to render enemy forces ineffective and unable to conduct operations . . . . Power plants shut down to avoid being bombed . . . . Such a strategy had been imagined by early airpower theorists but the requisite technology, particularly in the levels of precision attack, stealth, and information superiority, had not existed in previous conflicts.[95]

Overall, PPD20 directs by executive order, and without any congressional approval, the U.S. government to: (1) prepare counter-cyberattacks against foreign threat targets, and possibly contemplate preemptive cyberattacks for the sake of national security; (2) execute cyber operations within the United States, if

---

[91] PPD20, *supra* note 2, at 3.

[92] John Correll, *The Assault on EBO*, AIR FORCE MAGAZINE, Jan. 2013, at 52, *available at* http://www.airforcemag.com/MagazineArchive/Documents/2013/January%202013/0113EBO.pdf (explaining that the initial implementation of the concept in the successful Desert Storm air campaign led to formal recognition in the mid-1990s by the Joint Chiefs that EBO allowed the "effects of mass without the actual massing of forces").

[93] *See id.* (noting that before the traditionalist General James Mattis officially signed a rejection of EBO as head of the Joint Forces Command in 2008, other traditionalists had led a decade-long charge against the idea, such as the Army War College professor who lambasted EBO for its "overconfidence in the potential of technology").

[94] *Id.* at 54 ("The new Air Force Doctrine Document 3-0, Operations and Planning, will concentrate EBO, previously scattered through various doctrine documents, in a central location.").

[95] *Id.* at 52.

approved by the President or in an "Emergency Cyber Action," that could cause the destruction of American telecommunications infrastructure;[96] and (3) implement "cyber collection operations" (cyber espionage performed against other nations by the U.S. government).[97]

Despite the offensive capabilities PPD20 authorizes, the order is steeped in a legal caution that equates to rules of engagement at the strategic level. The order mandates that all cyber operations conform to the Constitution and "other applicable laws and policies of the United States . . . ."[98] Except in emergency situations, any domestic DCEO or OCEO activity undertaken by the government—activity that produces "cyber effects"—requires Presidential approval.[99]

B. *Collateral Damage and Cyberwar*

The language of PPD20 also involves another key military concept: collateral damage. The Department of Defense defines collateral damage as "unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time."[100] PPD20 considers collateral "consequences" rather than "damages" in admitting that "even for subtle or clandestine operations, [OCEO and DCEO] may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect *U.S. national interests in many locations*."[101] Similarly, PPD20 defines "significant consequences"—which PPD20 notes are possible with the conduct of OCEO and DCEO—as the "[l]oss of life, significant responsive actions against the United States,

---

[96] PPD20, *supra* note 2, at 6–7.

[97] PPD20, *supra* note 2, at 4. These collection operations are apparently sensitive and high-risk given that PPD20 states they are "reasonably likely to result in 'significant consequences.' " *Id*.

[98] *Id.* PPD20 also directs operational compliance with international law. *Id.*

[99] PPD20, *supra* note 2, at 6.

[100] JOINT CHIEFS OF STAFF, PUB. 1-02, DEP'T OF DEF. DICTIONARY OF MILITARY AND ASSOCIATED TERMS 41 (Oct. 15, 2013), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[101] PPD20, *supra* note 2, at 6 (emphasis added).

significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[102]

What PPD20 does not define, at least in its leaked form, are the specific actions the directive authorizes under the vaguely titled OCEO and DCEO. Based on a separate document the Washington Post obtained but did not publish, emergency operations would include those "necessary to mitigate an imminent threat or ongoing attack against U.S. national interests."[103] Leadership of organizations such as the National Security Agency ("NSA") have noted the rise of particular threats, such as DDoS attacks on the financial and energy sectors, in justifying increasing capabilities to confront them,[104] but they have not specified their doctrine of tactics. Accordingly, the precise actions PPD20 endorses are still unknown. Valuable targets will not only have sophisticated network defenses but also their own "incident response teams" to address standard attacks on their own.[105] If internal defenses fail, their response team would alert and coordinate with their respective internet service provider ("ISP"), such as AT&T, to implement mitigation techniques.[106] For example, in coordination with the ISP,[107] the victim can use a method known as "sinkhole" routing to temporarily divert the flood of DDoS traffic from normal communication, although in the case of a severe DDoS

---

[102] PPD20, *supra* note 2, at 3.

[103] Robert O'Harrow Jr. & Barton Gellman, *Secret cyber directive calls for ability to attack without warning*, WASH. POST (June 7, 2013), http://articles.washingtonpost.com/2013-06-07/world/39817439_1_cyber-tools-President-obama-directive.

[104] The leader of the NSA and its military counterpart, U.S. Cyber Command, during the launch of another force component, noted, "Look at what's happened in the past year. . . . Over 300 distributed denial-of-service attacks on Wall Street. We saw destructive attacks in August 2012 against Saudi Aramco and RasGas [Co. Ltd.]." Cheryl Pellerin, *Cybercom Activates National Mission Force Headquarters*, AMERICAN FORCES PRESS SERVICE (Sept. 25, 2013), http://www.defense.gov/news/newsarticle.aspx?id=120854.

[105] *See* Interview with Patrick McNeil, Certified Information Systems Security Professional, in Raleigh, N.C. (Oct. 16, 2013) [hereinafter McNeil]. His views are entirely his own.

[106] *See id.*

[107] If the DDoS is overseas, the ISP could be a non-American corporation. *See id.*

attack the only possible solution may be a "black hole" diversion that cuts off the network completely.[108] In addition, the ISP can work with the victim to locate and disable the command and control ("C&C") server of the DDoS.[109] These servers can themselves be unwitting zombies, hijacked to spread the DDoS to zombie computers without the knowledge of the server's owner, and also programmed to allow backup C&C servers to continue the DDoS assault if one C&C server is successfully turned off.[110]

Given that private entities ultimately address DDoS attacks, the most likely defensive execution of PPD20 by the NSA[111] could arise when an ISP does not act in a timely manner to shut off a DDoS attack.[112] If the NSA needs alacrity from a victim's ISP (an ISP unknowingly facilitating a zombie army or a C&C server) the NSA could either force their hand by the "law" of PPD20 or hack directly into the ISP if it is non-compliant with the PPD20-authorized order.[113] The NSA could also hack into the same

---

[108] *See* Charalampos Patrikakis, Michalis Masikos & Olga Zouraraki, *Distributed Denial of Service Attacks*, THE INTERNET PROTOCOL J., Dec. 2004, at 13, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/ipj_7-4.pdf (comparing the two route filter techniques as DDoS defenses).

[109] *See* Felix Leder et al., *Proactive Botnet Countermeasures An Offensive Approach*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 211, 214–15 (Christian Czosseck & Kenneth Geers eds., 2009) (summarizing how to disable a C&C server).

[110] *See* McNeil, *supra* note 105 (describing how sophisticated DDoS attacks can hijack hundreds of servers to command and control zombies, with zombies resorting to alternates if countermeasures take them down); *see also* Leder, *supra* note 109, at 215 ("Infected machines can also contain functionality to spread autonomously . . . .").

[111] As NSA is the most well-known of likely PPD20 executing arms of the United States Government, this Recent Development refers to the agency as a short-hand for any government agency executing the directive order.

[112] *See* McNeil, *supra* note 105 (adding that the NSA or the FBI could also work with ICANN, an international governing body of internet domain names to shut off the DDoS traffic to those names, but deciphering the "hundreds of permutations" of messages between zombies and C&C servers could be too time-consuming in an emergency).

[113] *See* McNeil, *supra* note 105 (noting the NSA's past decade of pressure on ISPs for other national security purposes).

hijacked zombie C&C server to shut it off remotely,[114] although that server, likely a small to medium sized organization such as a business, could then lose all ability to communicate.[115] Finally, the NSA could download zombie-bot removal tools without the owner's knowledge, doing so as quietly as the hacker installed the zombie bot,[116] although this tactic raises collateral concerns of ethics, legality, and liability,[117] as well as efficiency.[118]

All the above implications of the "collateral consequences" arise from the defense of just one type of attack. In order for the NSA to stop espionage or site hijacking, deterrence through its own cyberattacks, such as those outlined in PPD20, may be the government's primary option. OCEO and DCEO could permit the NSA to launch its own DDoS attack, initiate a virus, or use surveillance techniques to monitor private networks it believes are unable to prevent strategic espionage. Because the powerful language of PPD20 is vacuously strategic and void of tactical clarity, the power government operatives may exercise under PPD20 is open to speculation.

V. PPD20, THE SUPREME COURT, AND THE CONSENT OF CONGRESS

"The great office of President is not a weak and powerless one," wrote Justice Douglas as he joined a chorus of his colleagues

---

[114] *See* Leder, *supra* note 109, at 215 ("[C]ases are known where a botnet takeover was performed with the goal to issue commands that make the bots stop an attack or deinstall themselves. . . . Attacks are stopped immediately and the botnet is eventually shut down conclusively without the chance to be brought back up by the owner.").

[115] *See* McNeil, *supra* note 105 (referencing the many small to medium businesses typically victimized by similar attacks because they have servers advanced enough to be of use but lack the resources to defend themselves).

[116] *See* Leder, *supra* note 109, at 223 ("The most controversial discussion takes place about more invasive strategies, like a remote removal of bots from infected computers.").

[117] *See* Leder, *supra* note 109, at 222–24 (raising an ethical concern, a separate legal concern of downloading and running software without permission, and a liability concern from problems caused by the downloaded software).

[118] *Compare* Leder, *supra* note 109, at 222 (assessing the method as a "technically feasible" strategy to prevent harm), *with* McNeil, *supra* note 105 (noting that discovery of how the C&C network works is first required).

in establishing Presidential limits in *Youngstown Sheet & Tube Co. v. Sawyer*.[119] Powerful as the office may be, the Constitution fetters the Presidency in lawmaking, even when the President justifies executive orders on grounds of a national security necessity.[120] Although Article II of the Constitution vests the President with considerable powers in national security,[121] Article I precedes those clauses by enumerating the powers of Congress, which include not only legislative powers,[122] but also the province of raising armies,[123] supplying navies,[124] and declaring war.[125] The Court's decisions during President Bush's War on Terror proved its reluctance to give the Presidency a blank check in times of conflict.[126] But while the Court has limited the President's national security prerogative, the Court has also established a general deference to a President's *foreign policy* actions (as opposed to national security orders writ large) in *United States v. Curtiss-Wright Export Corp.*[127] The degree of that deference, which can hinge on the exigency of the particular dispute or judicial

---

[119] 343 U.S. 579, 633 (1952) (Douglas, J., concurring).

[120] *See generally* 343 U.S. 579 (rejecting President Truman's argument that the military's need for steel in the Korean War justified the seizure); *see also id.* at 587 ("Nor can the seizure order be sustained because of the several constitutional provisions that grant executive power to the President. In the framework of our Constitution, the President's power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker.").

[121] *See* U.S. CONST. art. II, § 2, cl. 1 (enumerating the commander-in-chief power and other military powers).

[122] U.S. CONST. art. I, § 1.

[123] *Id.* § 8, cl. 12.

[124] *Id.* § 8, cl. 13.

[125] *Id.* § 8, cl. 11.

[126] *See, e.g.*, Boumediene v. Bush, 553 U.S. 723 (2008) (rejecting the Military Commissions Act of 2006, which the President championed through Congress following the administration's previous failures to convince the Court to curtail rights to detainees in *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006), and *Rasul v. Bush*, 542 U.S. 466 (2004)).

[127] 299 U.S. 304, 320 (1936) ("[T]he very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations [is] a power which does not require as a basis for its exercise an act of Congress").

philosophy, is central to how far the President can act without Congress in his cyberwarfare strategy of PPD20.

A. Youngstown *and Congressional Support*

In *Youngstown*, steel companies took President Truman to court when he seized steel mills to prevent a union strike in the middle of the Korean War.[128] The steel companies argued, and the Supreme Court agreed, that Truman's executive order to seize the mills exceeded his constitutional authority as President.[129] The majority reasoned that the President needed congressional authorization for his purported seizure power.[130] Of the six opinions written in support of the holding, Justice Jackson's concurrence emerged to guide later decisions of similar inter-branch conflicts.[131] Justice Jackson reasoned that presidential actions fit into one of three categories, each encompassing a different degree of congressional support or opposition.[132] In the first category, no balance-of-powers protest is valid because Congress authorizes the power that the President exerts.[133] The second category occurs when Congress is silent, leaving the Presidential action in a "zone of twilight" where the authority to act is either concurrent or uncertain, and its constitutionality is

---

[128] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 583 (1952).

[129] *See id.* at 589.

[130] *See id.* at 585 ("The President's power, if any, to issue an order must stem either from an act of Congress or from the Constitution itself.").

[131] *See, e.g.*, Medellin v. Texas, 552 U.S. 491, 524 (2008) (employing "Justice Jackson's familiar tripartite scheme"); Dames & Moore v. Regan, 453 U.S. 654, 661 (1981) (noting a general agreement that Justice Jackson's concurrence "brings together as much combination of analysis and common sense as there is in this area").

[132] *See* 343 U.S. at 635 (Jackson, J., concurring) (framing these categories before assessing the facts of Truman's unilateral action).

[133] *See id.* ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. In these circumstances, and in these only, may he be said (for what it may be worth) to personify the federal sovereignty. If his act is held unconstitutional under these circumstances, it usually means that the Federal Government as an undivided whole lacks power.").

situation dependent.[134] The third category occurs when Congress has denied the power to the President, and the action is then constitutional only if Article II empowers the President to issue it.[135]

Congress has not addressed, and thus has not explicitly rejected, PPD20. Both the CFAA and the EEA deal with criminal recourses to hacking, while the PPD20 entails a military response and emphasizes compliance with U.S. domestic laws.[136] In addition, neither the CFAA nor the EEA can (effectively) criminalize state-sponsored hackers operating overseas,[137] leaving a gap in this area of vulnerability. The protective purpose of both laws arguably indicates implicit congressional support for executive action against foreign hacking.

On the other hand, the above indicia of congressional inaction and unspoken support may be insufficient for a finding of valid *authorization* outlined in Justice Jackson's first category. In *Youngstown*, Justice Jackson determined Truman's actions were not in the first category of his framework because, simply, "it is conceded that no congressional authorization exists for this seizure."[138] Similarly, no law, not the CFAA or the EEA, explicitly authorizes the President to create "cyber effects" through the same computer networks the President aims to use PPD20's operations to defend.

Because no law authorizes cyber effects, PPD20 falls into one of the other two categories. PPD20 may fall into the second category, the "zone of twilight" in which the President has acted "in absence of either a congressional grant or denial of authority."[139] "[C]ongressional inertia, indifference, or quiescence may sometimes, at least as a practical matter, enable, if not invite,

---

[134] *See id.* (explaining the second category).

[135] *See id.* at 637 (stating that when the President's actions contradict with the will of Congress, the President can then "rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter").

[136] PPD20, *supra* note 2, at 4.

[137] *See supra* Part III.

[138] 343 U.S. at 638.

[139] *Id.* at 635.

measures on independent presidential responsibility."[140] However, an analog to the specific facts of *Youngstown* and the Court's reasoning in the case is illustrative of the narrowness of this gray area between the branches.

In *Youngstown*, the Court decided that Truman could not commit an action proscribed by Congress in a manner differently than Congress authorized: "In choosing a different and inconsistent way of his own, the President cannot claim that it is necessitated or invited by failure of Congress to legislate upon the occasions, grounds and methods for seizure of industrial properties."[141] Three statutes were available to Truman for seizures to "supply the needs of the government itself," but instead he seized the mills by his own executive fiat.[142] Similar to those statutes, Congress has passed—and continues to debate—statutory means by which the executive branch may protect Americans in the field of cybersecurity.[143] Congress has deliberated upon the problem, and legislated the EEA and the CFAA as the solutions which the executive branch must carry out to protect America from cyber threats. In those deliberations, Congress does not authorize PPD20's "cyber effects operations" as a means to that end.

If Congress has not authorized PPD20 despite legislating the field of cybersecurity, PPD20 falls into the third of Justice Jackson's categories: a Congressional denial of authority. In alignment with Justice Jackson's logic, Justice Frankfurter interpreted a lack of authorization by Congress, in an area actively in its legislative purview, as a deliberate decision to *deny* the executive such authority.[144] Unlike the dissenters, the majority was not made any more sympathetic to the President by the silence on Capitol Hill following the seizures.[145] Congress has similarly

---

[140] *Id.* at 637.
[141] *Id.* at 639.
[142] *See id.* at 639.
[143] *See supra* Part III.
[144] 343 U.S. at 601–17 (Frankfurter, J., concurring) (finding a denial of power because Congress had deliberated upon which seizure powers to vest with the President in passing the Labor Management Relations Act of 1947).
[145] *Id.* at 675–77 (Vinson, J., dissenting) (noting both Congress's initial silence after President Truman messaged Congress the day following his order to

failed to sustain or reject the assertiveness of PPD20, remaining silent on the order because the document was leaked to the press over four months from the time of this writing.

These conclusions arise with caution. In *Youngstown*, multiple Justices in the majority noted that Congress had considered authorizing the power Truman employed, and had decided not to empower the President in this manner.[146] Thus, the Justices who ruled against Truman were addressing a deliberate use of executive power that Congress had specifically considered and rejected.[147] Accordingly, issuance of PPD20 contrasts with the steel seizure because Congress has never contemplated such a grant of authority in its deliberations.

Despite the caveat that Congress has not specifically addressed these (technically top secret) means of cybersecurity, an execution of PPD20 would likely fall into the third category, where a ruling of unconstitutionality would loom if challenged after any "collateral consequences." When the Court determines Congress has not authorized a Presidential action,[148] the Court has held that, rather than falling in the uncertain "zone of twilight," actions

---

explain his position, and once again, twelve days later, when Truman messaged the Senate and "described the purpose and need for his action and again stated his position that 'The Congress can, if it wishes, reject the course of action I have followed in this matter.' ").

[146] *See id.* at 639.

[147] Whereas Frankfurter focused on the Labor Management Relations Act of 1947, *see id.* at 601–17, Justice Black's majority opinion also noted how Congress had considered powers of seizure to assign the President in the Taft Hartley Act, and specifically rejected an amendment for seizure powers in times of national emergency. *See id.* at 586 ("Apparently it was thought that the technique of seizure, like that of compulsory arbitration, would interfere with the process of collective bargaining.").

[148] The case of *Dames & Moore v. Regan*, 453 U.S. 654 (1981), is instructive (but also exceptional) on how far the Court will go to interpret congressional support rather than adjudicate a "zone of twilight." In that case, the Court, facing a tight deadline and a silent Congress, upheld an executive order by interpreting "three not-quite-applicable pieces of legislation" as implicitly signaling congressional support for the President's executive order. *See* KENNETH R. MAYER, WITH THE STROKE OF A PEN: EXECUTIVE ORDERS AND PRESIDENTIAL POWER 57 (2002) (quoting HAROLD KOH, THE NATIONAL SECURITY CONSTITUTION 48 (1990)).

subject to *Youngstown* analysis that violate the "implied will" of Congress fall into Jackson's third category.[149]

B. *The Power of the President in Foreign Affairs:* Curtiss-Wright*'s Lasting Dicta*

In contrast to *Youngstown*, *United States v. Curtiss-Wright Export Corporation*[150] was not a dispute about the President's power to act unilaterally without Congress, but instead about how much power Congress could constitutionally delegate to the executive.[151] Rather than criminalize sales by American arms manufacturers to combatants in Bolivia, Congress chose to empower the President to criminalize such sales at his discretion.[152] Although the Court had recently rejected Congressional delegation of legislative power to President Roosevelt in New Deal legislation,[153] Justice Sutherland held that this matter differed because the delegation was in foreign policy.[154] Justice Sutherland

---

[149] *See* Medellin v. Texas, 552 U.S. 491, 528 (2008) (establishing a high bar for "congressional acquiescence" of the second *Youngstown* category, and overruling the President's actions to implement a non-self-executing treaty in part because they did not overcome that bar after "Congress's failure to act following the President's resolution").

[150] 299 U.S. 304 (1936).

[151] *Id.* at 315 ("The determination which we are called to make, therefore, is whether the Joint Resolution . . . is vulnerable to attack under the rule that forbids a delegation of the law-making power.").

[152] *Id.* at 311–12 ("[An] indictment . . . charges that appellees . . . conspired to sell in the United States certain arms of war, namely fifteen machine guns, to Bolivia . . . in violation of the Joint Resolution of Congress . . . and the provisions of a proclamation issued on the same day by the President of the United States. . . . The Joint Resolution . . . follows: . . . 'That if the President finds that the prohibition of the sale of arms and munitions . . . may contribute to the reestablishment of peace between those countries, and . . . he makes proclamation to that effect, it shall be unlawful to sell . . . until otherwise ordered by the President or by Congress.' ").

[153] *See, e.g.*, Schechter Poultry Corp. v. United States, 295 U.S. 495, 537–38 (1935) ("Congress cannot delegate legislative power to the President to exercise an unfettered discretion to make whatever laws he thinks may be needed or advisable for the rehabilitation and expansion of trade or industry.") (citing Panama Refining Co. v. Ryan, 293 U.S. 388 (1935)).

[154] 299 U.S. at 315 ("[W]e [should] first consider the differences between the powers of the federal government in respect of foreign or external affairs and

held that foreign and domestic policies are "two classes of power . . . different, both in respect of their origins and their nature."[155]

This fundamental difference between foreign and domestic affairs meant that "legislation . . . must often accord to the President a degree of discretion and freedom from statutory restriction which would not be admissible were domestic affairs alone involved."[156] However, Justice Sutherland went further than to simply adjudicate the issue of delegation, explaining in extensive dicta how the President's power in foreign relations is so inherent in America's sovereignty that it rests on neither law nor the Constitution.[157] Sutherland believed this sovereign power to conduct foreign affairs passed to the Presidency from the British monarchy upon independence, and, in quoting Chief Justice John Marshall, that the Framers supported this view of the President's preeminence abroad.[158] Paraphrasing Marshall, Sutherland concluded with regards to the issue before the court, "we are here dealing not alone

---

those in respect of domestic or internal affairs. That there are differences between them, and that these differences are fundamental, may not be doubted.").

[155] *Id.*

[156] *Id.* at 320; *see also id.* at 315 (noting the constitutionality of the delegation may have been different had it "related solely to internal affairs" but that because it did not, the Court finds the question "unnecessary to determine").

[157] *Id.* at 315–16 ("The broad statement that the federal government can exercise no powers except those specifically enumerated in the Constitution, and such implied powers as are necessary and proper to carry into effect the enumerated powers, is categorically true only in respect of our internal affairs.").

[158] Justice Sutherland explains that sovereignty passed upon the United States as a whole upon America's peace treaty with Great Britain. *Id.* at 317. Accordingly, in his view, this inherent power fell to the President because the Framers and their immediate predecessors had resolved that the President is "the constitutional representative of the United States with regard to foreign nations." *Id.* at 320 (quoting "[t]he Senate Committee on Foreign Relations at a very early day in our history (Feb. 15, 1816)" (U.S. Senate, Reports, Committee on Foreign Relations, vol. 8, p. 24)). Justice Sutherland's reasoning culminates in the words of John Marshall: "As Marshall said in his great argument of March 7, 1800, in the House of Representatives, 'The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations.' " *Id.* at 319 (internal citation omitted).

with an authority vested in the President by an exertion of legislative power, but with such an authority plus the very delicate, plenary and exclusive power of the President as the *sole organ of the federal government in the field of international relations* . . . ."[159] The sum of his reasoning—in dicta—is an elevation of the President's power to conduct foreign policy beyond the restraints of Congress,[160] and possibly even the Constitution.[161]

Scholarly criticism of Justice Sutherland's *Curtiss-Wright* opinion is legion, due both to contention with the historical support underpinning Sutherland's reasoning[162] and the presidential

---

[159] *Id.* at 319–20 (emphasis in original).

[160] Justice Sutherland states, prior to introducing John Marshall's "sole organ" speech on the floor of the House of Representatives, that Congress and the President are not equals in America's negotiations with foreign powers. *Id.* at 319 ("In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation. He *makes* treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it.") (emphasis in original).

[161] Justice Sutherland concluded that the President's ability and right to conduct foreign policy rested on American sovereignty, not the Constitution. *Id.* at 318 ("[T]he investment of the federal government with the powers of external sovereignty did not depend upon the affirmative grants of the Constitution. The powers to declare and wage war, to conclude peace, to make treaties, to maintain diplomatic relations with other sovereignties, if they had never been mentioned in the Constitution, would have vested in the federal government . . . ."). Justice Sutherland reasoned these powers could be extra-constitutional. *See supra* note 157 and accompanying text.

[162] In regard to how Justice Sutherland reversed the meaning of the 'sole organ' quote from then-Congressman John Marshall, *see, e.g.*, Joel R. Paul, *The Geopolitical Constitution: Executive Expediency and Executive Agreements*, 86 CALIF. L. REV. 671, 690 ("Marshall was defending President Adams' request for extradition of a British subject pursuant to the Jay Treaty . . . . Clearly, Marshall meant that the President was bound by law to carry out treaties. Far from asserting the executive's discretion in foreign relations, Marshall characterized the executive as the agent or 'organ' of Congress. Sutherland twisted Marshall's statement to support the contrary proposition—that the President's foreign relations powers were plenary and neither derived from, nor were limited by, Congress."). In regard to Justice Sutherland's (mis-)understanding of the Framers' support for his expansive view of Presidential prerogative, see

empowerment that flowed from the holding.[163] However, the words of dicta—neatly encapsulated in the "sole organ" language—continue to guide the Court's jurisprudence when questions surface of presidential power abroad. Most recently, the Court applied *Curtiss-Wright* in *Pasquantino v. United States*.[164] The litigants in *Pasquantino*[165] argued that the federal wire fraud statute cannot be used to prosecute those attempting to defraud a foreign government of that government's rightful tax revenue.[166] The Court disagreed with this narrow view of the statute's application, holding that the executive branch was well within its scope of authority.[167] The holding did not rest on *Curtiss-Wright*,

---

HAROLD KOH, THE NATIONAL SECURITY CONSTITUTION 72, 74 (1990) ("Framers rejected the option of centralizing the national government's foreign affairs powers in the President alone. . . . To the contrary, the Framers fully intended them to apply to both foreign and domestic affairs."). *See also id.* ("Every grant to the President . . . relating to foreign affairs, was in effect a derogation from Congressional power, eked out slowly, reluctantly, and not without limitations and safeguards.") (quoting LOUIS HENKIN, FOREIGN AFFAIRS & THE CONSTITUTION 56–65 (1972)).

[163] *See* Louis Fisher, *National Security Law: The Judicial Role*, *in* FREEDOM AND THE RULE OF LAW 201, 205 (Anthony A. Peacock, ed. 2009) ("Of all the misconceived and poorly reasoned judicial decisions that have inflated presidential power in the field of national security, confused the judiciary, weakened the rule of law, and endangered individual rights, *Curtiss-Wright* stands in a class by itself.").

[164] 544 U.S. 349, 351 (2005) ("This action was brought by the Executive, 'the sole organ of the federal government in the field of international relations,' *United States v. Curtiss-Wright Export Corp*. . . . [I]t may be assumed that by electing to prosecute, the Executive has assessed this prosecution's impact on this Nation's relationship with Canada, and concluded that it poses little danger of causing international friction."). *See also id.* at 369 (supporting the rejection of petitioners' claims of federal overreach once more with reference to *Curtiss-Wright*'s "sole organ" principle).

[165] These defendants were modern rum-runners; they "were indicted for and convicted of federal wire fraud for carrying out a scheme to smuggle large quantities of liquor into Canada from the United States." *Id.* at 353.

[166] *Id.* ("Petitioners contended that the Government lacked a sufficient interest in enforcing the revenue laws of Canada, and therefore that they had not committed wire fraud.").

[167] *Id.* at 372 ("It may seem an odd use of the Federal Government's resources to prosecute a U.S. citizen for smuggling cheap liquor into Canada. But the

but "Justice Thomas' casual citation of the 'sole organ' language [in the majority opinion] suggests that there is still broad support on the Court for strong deference to the President for all matters involving foreign affairs."[168]

The impact of *Curtiss-Wright* on future constitutional challenges to executive action is uncertain, in large part because its impact in case law is so unclear. For Harold Koh, former Dean of Yale Law School, the dicta now unofficially embodies one of two philosophical poles of constitutional interpretation pertaining to national security, with *Youngstown*'s mandate of "congressional concurrence in most decisions on foreign affairs" representing the opposing pole. *Curtiss-Wright*, in contrast, "fully and officially crystalize[d]" a philosophical embrace of unfettered executive discretion in foreign affairs.[169]

However, other scholars have embraced an entirely separate distinction between *Youngstown* and *Curtiss-Wright*, namely, that the former was not a foreign affairs decision at all.[170] The historian Arthur Schlesinger and the foreign affairs legal scholar Louis Hencken hold the view that *Youngstown* is a case of domestic policy,[171] and that perspective emerges from the opinion itself. Justice Jackson's concurrence implied a president's foreign affairs

---

broad language of the wire fraud statute authorizes it to do so, and no canon of statutory construction permits us to read the statute more narrowly.").

[168] Julian Ku, *Curtiss-Wright is Back: The President as the "Sole Organ of Foreign Affairs,"* OPINIO JURIS (Apr. 29, 2005, 2:51 PM), http://lawofnations.blogspot.com/2005/04/curtiss-wright-is-back-president-as.html.

[169] *See* KOH, *supra* note 162.

[170] Stephen Griffin, *A "Domestic" Case? Mysteries of Youngstown*, BALKINIZATION (Oct. 10, 2008, 1:43 PM), http://balkin.blogspot.com/2008/10/domestic-case-mysteries-of-youngstown.html (noting scholarship framing *Youngstown* as a case of domestic policy despite President Truman's national security necessity arguments).

[171] *See id.* (quoting Schlesigner's conclusion that "neither the majority nor even the minority [in *Youngstown*] saw the case as involving in any primary sense the President's authority in foreign affairs."); *see also id.* (quoting Henkin's similar conclusion that "Youngstown has not been considered a 'foreign affairs case.' The President claimed to be acting within 'the aggregate of his constitutional powers,' but the majority of the Supreme Court did not treat the case as involving the reach of his foreign affairs power.").

conduct was permissibly "largely uncontrolled" and "unknown," but that such prerogative could not allow the President to "vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign adventure."[172] Backing this view, the Court, in a concurrence signed by four Justices, has explicitly contrasted the *Youngstown* domestic policy rationale with the foreign affairs underpinning of *Curtiss-Wright*.[173]

Geographic location of PPD20 actions would then become critical. PPD20 authorizes actions in cyberspace, but cyberspace, while global and conceptually ethereal, exists inside physical objects, "hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work."[174] This physical reality of cyberspace underscores the dangers that PPD20 endeavors to confront:

> By definition, cyberattacks are directed against computers or networks. . . . Attackers can target computer chips embedded in other devices, such as weapons systems, communications devices, generators, medical equipment, automobiles, elevators and so on. . . . Another target can be the computing systems controlling elements of the nation's critical infrastructure. For example, the electric power grid, the air traffic control system, the transportation infrastructure, the financial system, water purification and delivery and telephony rely on controllers. . . . Finally, attackers can target dedicated computing devices such as desktop or mainframe computers in particular sensitive offices, or in critical operational software used in corporate or government computer centers.[175]

PPD20's virtual battlefield exists throughout those pieces of hardware and the bandwidth they need to communicate the

---

[172] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 642 (1952).

[173] Goldwater v. Carter, 444 U.S. 996, 1004 (1979) (Rehnquist, J., concurring) (contrasting *Youngstown*, where private parties challenged "an action of profound and demonstrable domestic impact" to the case at bar, that mirrored *Curtiss-Wright* as it was "entirely external to the United States [and] within the category of foreign affairs").

[174] Reveron, *supra* note 1, at 5.

[175] Herbert Lin, *Operational Considerations in Cyber Attack and Cyber Exploitation*, *in* CYBERSPACE AND NATIONAL SECURITY 3, 38 (Derek Reveron, ed., 2012).

invaluable information of modern computer networks. The critical issue for PPD20's constitutionality could then rest on where its authorized operations occur.

The constitutionality of PPD20 is in question because Congress has not taken a position on PPD20 and because the geographic range of PPD20 is unclear. Because Congress has not expressly authorized PPD20, the constitutionality of the President's power could hinge on whether PPD20 execution falls squarely into the President's foreign affairs conduct.

VI. APPLICATION OF PRECEDENT TO POSSIBLE PPD20 SCENARIOS

Consider the following hypothetical. The National Security Agency ("NSA") discovers Comment Crew's trespass into a particularly sensitive area of national security: a weapon development project at Northrup-Grumman.[176] Authorized by the OCEO framework, the NSA launches a sophisticated DDoS strike against the computers from which the Comment Crew operates to overload Comment Crew computers, all of which the NSA has listed as targets under the guidance of PPD20. The NSA endeavors to tie up the Chinese with the DDoS flood long enough to cut off the incursion and secure its American target from another breach. But the attack, powered by NSA and their willing zombies in U.S. Cyber Command,[177] proves overwhelming. Financial centers in Shanghai stagger, unable to conduct the routine transactions necessary for banking. In response, Chinese hackers launch their own DDoS attacks against Wall Street institutions, escalating a cyberwar. The American public and many members of Congress fulminate; they question how the President's OCEO could trigger this result due to a small cyberattack on a defense

[176] Northrop Grumman is a long-time military aerospace manufacturer and weapons researcher; its heritage of research and production includes the B2 Stealth Bomber. *See About Us — Our Heritage*, NORTHROP GRUMMAN, http://www.northropgrumman.com/AboutUs/OurHeritage/Pages/default.aspx (last visited Oct. 19, 2013).

[177] The degree of coordination between U.S. Cyber Command and the NSA is such that Army General Keith Alexander helms both organizations. *See* Pellerin, *supra* note 104.

contractor when Congress never authorized the method of cybersecurity, let alone an unprecedented Internet war.

Presuming their DDoS never commandeered—"zombified"—private American computers, this hypothetical counterattack against the Chinese hackers would likely be constitutional, despite any barrage of criticism from Congress after the fact. Because the executed OCEO remained under the umbrella of foreign affairs, the distinction between foreign and domestic affairs could save the action under the "plenary and exclusive power of the President . . . in the field of international relations" established in *Curtiss-Wright*.[178] If the dicta of *Curtiss-Wright* influences the Court in a handling of a PPD20 matter more so than Justice Jackson's concurrence, congressional support may be unneeded.

The constitutionality of PPD20 might be less certain if the geographic location of the activity were determined to be domestic. For example, the physical location of the President's DCEO and OCEO might be the networks, servers, routers, and laptops in the United States. Consider a second scenario subsequent to the one above: Sino-American tensions have abated from their apex but continue to simmer. When another debt ceiling deadline looms in Washington, Beijing is eager to undermine the American dollar in global markets. Using the information gathered from the Comment Crew, China successfully hacks into Bank of America's ("BoA") systems to respectively turn its servers and thousands of computers into C&C servers and zombies. BoA's zombies crash major media outlets and the laptops and email servers on Capitol Hill and at the White House as America's elected officials neared a debt ceiling compromise in eleventh hour negotiations. The FBI rushes to contact BoA, but cannot reach the bank due to the sophistication of the attack in crashing email and phone lines. Under PPD20, the NSA decides shutting off BoA from the world is the lesser of two evils, and the President concurs. The ISP is disinclined to shut off BoA without waiting for their customer's consent because BoA's computers' content and transactions were unaffected by zombie takeover; the ISP relents when the NSA effectively seizes their operations based on the powers of PPD20.

[178] *See supra* note 158 and accompanying text.

The NSA then "blackholes" BoA's network after tracking some zombies' C&C servers, which the NSA disables through coercive measures taken with the ISP.

No matter the success or popularity of the President's repulsion of a deliberate attack, the President's actions may have exceeded the scope of his constitutional authority. If BoA or its ISP challenged the government's actions, they would share the plaintiffs' position in *Youngstown*. The President could only justify this domestic execution of PPD20 actions if Congress had endorsed the seizure. Just as in *Youngstown*'s analysis of seizure statutes, the test of congressional support would be whether or not Congress had addressed the field, and if so, had it authorized the means in question. Assuming Congress has failed to do so, under this domestic implementation, the actions would fall into *Youngstown*'s third category. The President would have to prove that Article II of the Constitution permits him, without Congressional support, to fight a cyberwar with "collateral consequences" over domestic computer networks.

VII. CONCLUSION

If the President recedes from his foreign affairs conduct into domestic affairs and directs cyber operations to defend American computer networks, he may need an act of Congress. Congress could endorse the cyber war measures of PPD20 and make these issues moot. Without congressional approval, PPD20 could become an unconstitutional exercise of power if those operations went through private American computer networks and entailed inimical consequences on American lives and property.