John Gallagher

12/13/2017

Comp 116 – Computer Security

Ming Chow

Networks at War: Using Case Studies to Speculate About Potential Cyberattacks on Vital Infrastructure During Wartime

Abstract

During the Second World War, the last armed conflict between advanced economies, the Internet was nonexistent and electronic global communication networks were in their infancy.[1] In the years since the end of the Second World War, global telecommunications networks, namely the Internet, have become the bedrock of the world economy by facilitating the vast quantities of transcontinental transactions that underpin global trade. Beyond their economic implications, telecommunications, and especially the Internet, have also increased global communication in ways too numerous to mention, tying people across the world together. And though the years since the Second World War have seen no shortage of turmoil around the globe, the Internet developed into a cornerstone of global economy and society during a period free of open war between technologically advanced nations.

But given the increased geo-political tension between some of the world's major economic and military powers, the possibility of a future war between technologically advanced, Internet-dependent nations, while remote, is certainly worth considering. It is a near-certainty the Internet would play a vital role in such a conflict, but given that the Internet did not exist during the last armed conflict between technologically advanced nations, it is difficult to infer directly from history what the Internet's role

[1] Quora Contributor and Rebecca Onion, "Was It Possible to Make a Phone Call From Germany to the U.S. in 1946?," Slate, November 14, 2014, http://www.slate.com/blogs/quora/2014/11/14/was_it_possible_to_make_a_phone_call_from_germany_to_the_u_s_in_1946.html

might be. Though wartime cyberattacks could take many forms, this paper will speculate about potential attacks against infrastructure and to ground this speculation in reality, this paper will examine relevant contemporary case studies, including Russian cyberattacks in Eastern Europe and WannaCry's impact on Britain's National Health Service. Each of these case studies will provide insight into the role the Internet might play in a future war and thus inform citizens and governments about the kinds of scenarios they may face when the Internet is but one theatre of a wider war.

To the Community

Cyber warfare has become a hot-button issue in the American press over the past 18 months, perhaps in part due to Russian interference in the 2016 election, interference that was allegedly carried out via manipulation of social media.[2] There have been other notable cyber-attacks carried out by nation states that have received significant media coverage; the various Russian attacks in Eastern Europe, and the WannaCry ransomware, which leveraged stolen NSA exploits to devastating effect during the summer of 2017, are just two of many high profile cases.[3] When we consider the scale and frequency of state-sponsored cyberattacks, it is clear that we live in a world of perpetual low-grade cyber warfare, where the impact of government-sponsored cyberattacks is plainly evident.

Given that government-sponsored cyberattacks are so impactful in peacetime, what shape might cyber war take as a component of a wider war between Internet-dependent nations? While wartime cyberattacks could take almost any form, it doesn't take a quantum leap to see the propaganda potential

---

[2] Scott Shane, "The Fake Americans Russia Created to Influence the Election," The New York Times, September 7, 2017, sec. Politics, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

[3] Sheera Frenkel, "Global Ransomware Attack: What We Know and Don't Know," The New York Times, June 27, 2017, sec. Technology, https://www.nytimes.com/2017/06/27/technology/global-ransomware-hack-what-we-know-and-dont-know.html

Dan Goodin, "Hackers Trigger yet Another Power Outage in Ukraine," Ars Technica, January 11, 2017, https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/

of social media for instance. This paper will focus on the most tangible of potential wartime cyberattacks: attacks against infrastructure. Although such informed speculation is necessarily imprecise until vindicated or contradicted by an actual war, speculation based on reasonable case studies might help citizens and governments prepare for the eventuality of the Internet as one theater in a wider war.

Introduction: Cyberwar as a Component of Full-Scale War and The Potential For Future Conflict

There has been no open conflict between technologically advanced economies since the Second World War, and as such two heavily networked nations have ever been at war. The brief 2008 war between Russia and Georgia was "was the first time a known cyberattack had coincided with a shooting war."[4] Before armed hostilities began, DDoS attacks were carried out against Georgian targets and Georgian government websites were defaced.[5] Though these attacks were doubtless disruptive, the destructive potential of cyberattacks against Georgia in 2008 was limited because Georgia's infrastructure was not heavily dependent on the Internet. At the time of the war, *The New York Times* remarked:

> "[Georgia] ranks 74th out of 234 nations in terms of Internet addresses, behind Nigeria, Bangladesh, Bolivia and El Salvador ... Cyberattacks have far less impact on such a country than they might on a more Internet-dependent nation, like Israel, Estonia or the United States, where vital services like transportation, power and banking are tied to the Internet."[6]

We can infer from the 2008 Russo-Georgian War that, in future wars cyberattacks likely precede and accompany armed combat. But, given Georgian infrastructure's relative lack of dependence on the

[4] John Markoff, "Before the Gunfire, Cyberattacks," The New York Times, August 12, 2008, sec. Technology, https://www.nytimes.com/2008/08/13/technology/13cyber.html
[5] Ibid
[6] Ibid

Internet in 2008, the Russo-Georgian war does not provide much insight into the role the Internet might play in a longer conflict between two thoroughly Internet dependent nations.[7]

Such a conflict between two Internet-dependent nations is also no longer a distant hypothetical. North Korea's rapidly developing nuclear program is a geo-political tinderbox, and increased Chinese assertiveness in the South China Sea has put China at odds with its neighbors.[8] The United States' diplomatic capabilities have been compromised by a shortage of mid-level diplomats and regional experts at the State Department and the current U.S. President's is also an unpredictable actor in foreign affairs, who has been sharply criticized for exacerbating international crises via Twitter insults.[9]

In sum, we can see from the Russo-Georgian war that the Internet will almost certainly play a vital role in any future conflict between Internet-dependent nations. It is also clear that war between Internet-dependent nations is not so unlikely a prospect that it can be dismissed out of hand. Further, As the Russo-Georgian war does not provide good insight into the role that the Internet might play in a war between Internet-dependent nations, we instead must reach for alternative case studies that illustrate potential wartime cyberattacks on infrastructure.

---

[7] Ibid

[8] Choe Sang-Hun, "North Korea's New Missile Is Bigger and More Powerful, Photos Suggest," The New York Times, November 30, 2017, sec. Asia Pacific, https://www.nytimes.com/2017/11/30/world/asia/north-korea-missile-test.html
Chris Buckley, "Beijing Warns U.S. Over Navy Patrol in South China Sea," The New York Times, August 11, 2017, sec. Asia Pacific, https://www.nytimes.com/2017/08/11/world/asia/south-china-sea-trump-navy-patrol.html

[9] Choe Sang-Hun, "Kim's Rejoinder to Trump's Rocket Man: 'Mentally Deranged U.S. Dotard,'" The New York Times, September 21, 2017, sec. Asia Pacific, https://www.nytimes.com/2017/09/21/world/asia/kim-trump-rocketman-dotard.html

The Internet as a Weapon I - Attacks on Industrial Control Systems

Internet-connected infrastructure would likely be a priority target in the event of a war between Internet-dependent nations, not only because of the potential for massive disruption, but also because many of the industrial control systems that are the foundation of vital infrastructure are connected to the Internet and publicly visible. For instance, Shodan, a search engine for Internet-connected devices, lists numerous industrial control systems, from traffic lights to power plants.[10] In one instance in 2013, researchers were able to access a control panel for a hydro-electric power plant.[11] The control panel included the option to turn off a turbine - obviously functionality that should not have been publicly accessible.[12]

Shodan researchers argue that the main reason that industrial control systems are put online is to reduce costs by allowing technicians to manage these systems remotely.[13] While Shodan's researchers also maintain that there is "right" way to put an industrial control system online, given the sheer number of industrial control systems visible on Shodan, it is reasonable to conclude that many industrial control systems that drive vital infrastructure are insufficiently hardened to withstand attacks from capable and determined adversaries.[14]

Crippling attacks on vital industrial control systems are not only the provenance of doomsaying security researchers. Such attacks have occurred have occurred in the real world. For instance, in 2015 and 2016 attackers with suspected ties to Russia attacked Ukrainian power plants, briefly disabling

[10] David Goldman, "Shodan Finds the Internet's Most Dangerous Spots," CNNMoney, May 1, 2013, http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/
[11] Ibid
[12] Ibid
[13] "Map of Industrial Control Systems on the Internet " - accessed December 12, 2017, https://icsmap.shodan.io/
[14] Ibid

them.[15] The attackers disabled the power plants in 2016 by deploying malware dubbed "Crash Override" by security researchers.[16] "Crash Override" operates by manipulating low-level protocols used to manage industrial control systems, which is possible because these protocols were never intended to be secure as they were designed long before the notion of Internet-connected industrial control systems.[17]

Poorly-secured civilian industrial control systems are not the only potential targets of wartime cyberattack, as industrial control systems also power military infrastructure. 2009's Stuxnet was a complex and highly sophisticated piece worm designed to damage the centrifuges at an Iranian Uranium enrichment facility.[18] Stuxnet accomplished its goal of damaging the centrifuges by compromising the Siemens industrial control systems that powered them.[19] Stuxnet damaged the centrifuges by "subtly [changing] the motor-control frequencies that drive the centrifuges, thus affecting their spin rate and accelerating them to the point where they became unstable and failed."[20] Stuxnet was also reportedly able to remain undetected by sending falsified information to the infected ICS' system performance display.[21] The impact of this subtle manipulation was profound, Iran is estimated to have replaced 1000 centrifuges

[15] Dan Goodin, "First Known Hacker-Caused Power Outage Signals Troubling Escalation," Ars Technica, January 4, 2016, https://arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/
Dan Goodin, "Hackers Trigger yet Another Power Outage in Ukraine," Ars Technica, January 11, 2017, https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/
[16] Dan Goodin, "Found: 'Crash Override' Malware That Triggered Ukrainian Power Outage," Ars Technica, June 12, 2017, https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/
[17] Ibid
[18] Lucas Kello, ed., "The Quest for Cyber Theory," in The Virtual Weapon and International Order (Yale University Press, 2017), 23–57, http://www.jstor.org.ezproxy.library.tufts.edu/stable/j.ctt1trkjd1.6
Isaac R. Porche, Jerry M. Sollinger, and Shawn McKay, eds., "A Cyberworm That Knows No Boundaries," in A Cyberworm That Knows No Boundaries (RAND Corporation, 2011), 1–18, http://www.jstor.org.ezproxy.library.tufts.edu/stable/10.7249/op342osd.8
[19] Porche, Sollinger, McKay "A Cyberworm That Knows No Boundaries", 7
[20] Ibid
[21] Ibid

in a three month period at one of the affected enrichment facilities.[22] Overall, some observers estimate that Stuxnet set Iran's nuclear program back years.[23]

Given the existence of Stuxnet, an expensive to produce software artifact of such sophistication, that it could only have been produced by a nation-state, it is reasonable to conclude that states have already expended significant effort and resources to produce cyber-weapons that are effective against hardened ICSs.[24] Further, the success of Stuxnet illustrates that even industrial control systems in hardened facilities can be compromised by capable, determined, and well-resourced adversaries.

As many insecure industrial systems are already publicly visible on the Internet and malware already exists that targets them, it is reasonable to conclude that, should a war between Internet-dependent nations occur, insecure, Internet-connected industrial control systems would be a prime target for belligerents. As, if belligerents were to attack vulnerable industrial control systems with the intent to cause lasting harm, there is potential for Biblical disruption, as all manner of essential infrastructure civilian could be disabled. Furthermore, Stuxnet demonstrates that states can already combine the technical sophistication necessary to produce malware like Stuxnet with the espionage capability to deploy such malware to air-gapped facilities. Therefore, even hardened industrial control systems are not proof against wartime cyberattack. Given that both civilian and military industrial control systems are vulnerable, governments and civilians should expect the services that rely on ICSs to be disrupted to some extent during wartime.

The Internet as a Weapon II - Attacks on Vital Services

Insecure industrial control systems are not the only vulnerable infrastructure that attackers could target to undermine a nation's infrastructure. Garden-variety desktop PCs also undergird vital

[22] Ibid
[23] Ibid
[24] Ibid

infrastructure. For instance, Britain's National Health Service depends on everyday Windows machines for mundane administration. As a result, the NHS was badly impacted in 2017 by "WannaCry" a ransomware worm that encrypts data on infected systems and demands a ransom paid in Bitcoin to decrypt the files.[25] WannaCry is built on a Windows exploit called "Eternalblue" that was stolen from the NSA and made publicly available by a group known as Shadow Brokers.[26]

WannaCry disrupted thousands of appointments at dozens of NHS facilities across England as these facilities were unable to access patient data.[27] Lax security practices were the root cause of the problem, as WannaCry only impacted only those NHS facilities using unsupported or unpatched versions of Windows (Microsoft fixed the Eternalblue exploit in a March 2017 patch).[28] Though WannaCry was built based on an exploit discovered by the NSA, WannaCry has been attributed to North Korea.[29] WannaCry's demand for a ransom marks it as an attempt to obtain currency (a hallmark of North Korea's recent cyberattacks which generate millions of dollars for the regime) rather than a cyberweapon designed to cause maximum devastation.[30] Nevertheless, the disruption that WannaCry caused to the NHS demonstrated that a state-sponsored attack on commercial operating systems could be absolutely devastating to vital services.

---

[25] Dan Goodin, "An NSA-Derived Ransomware Worm Is Shutting down Computers Worldwide," Ars Technica, May 12, 2017, https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/

[26] Ibid

[27] Rory Cellan-Jones, "NHS Trusts 'at Fault' over Cyber-Attack," BBC News, October 27, 2017, sec. Technology, http://www.bbc.com/news/technology-41753022

[28] Goodin, "An NSA-Derived Ransomware Worm Is Shutting down Computers Worldwide"
Kat Hall 27 Oct 2017, "NHS Could Have 'Fended Off' WannaCry by Taking 'Simple Steps' – Report," accessed December 13, 2017, https://www.theregister.co.uk/2017/10/27/nhs_could_have_fended_off_wannacry_says_nao_report/

[29] Choe Sang-Hun, "North Korea Tries to Make Hacking a Profit Center," The New York Times, July 27, 2017, sec. Asia Pacific, https://www.nytimes.com/2017/07/27/world/asia/north-korea-hacking-cybersecurity.html

[30] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.," The New York Times, October 15, 2017, sec. Asia Pacific, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

As can be seen from the disruption WannaCry caused to the NHS, belligerents need not craft attacks on specialized systems to wreak national havoc, instead compromising vulnerable desktop computers is potentially just as devastating as compromising a power plant. The potentially lethal implications of delayed medical care are obvious and thus we can conclude that medical services will be prime targets of wartime cyberattacks. Other vital government services that depend on commercial desktop computers are also likely targets of such attacks.

The Internet as a Weapon III – Attacks on Private Companies

State-run services are not the only potential targets of wartime cyberattacks, as cyberattacks on private companies could also cause massive disruption. For instance, the United States has a massive domestic arms industry, where huge private companies such as Lockheed Martin and Northrop Grumman produce weapons systems for the various branches of the United States Military.[31] These companies are already subject to regular cyberattacks, some of which are believed to be state-sponsored, although company officials have been reluctant to directly attribute these attacks to any particular nation.[32] Given the tremendous military importance of these companies, in wartime, one can reasonably expect that attacks against defense firms will increase in frequency and sophistication.

One case study that provides some insight into the type of damage that a successful state-sponsored attack on a private enterprise might cause is North Korea's 2014 attack on Sony Pictures. In an attempt to stop the release of a satirical film "The Interview," a group calling itself "Guardians of Peace" gained access to Sony's Pictures' network and massively disrupted the company's operations.[33] Three-

---

[31] "The Three Largest Defense Companies in the World Are," accessed December 19, 2017, https://web.stanford.edu/class/e297a/U.S.%20Defense%20Industry%20and%20Arms%20Sales.htm#_edn2

[32] "U.S. Defense Firms Face Relentless Cyberattacks," Reuters, September 7, 2011, https://www.reuters.com/article/us-aero-arms-summit-cybersecurity/u-s-defense-firms-face-relentless-cyberattacks-idUSTRE7867F120110907

[33] Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm," The New York Times, December 30, 2014, sec. Media,

quarters of Sony's servers were destroyed during the attack and vast troves of confidential data were publicly released in multiple document dumps, which caused deep embarrassment to Sony executives.[34] The damage caused by the attack meant that employee access to Sony's computer systems was disrupted for weeks after the attack had taken place.[35] Although one could argue that Sony Pictures is of limited national security significance, after Sony decided to cancel the theatrical release of the "The Interview" the company drew intense criticism, then U.S. President Obama even weighed in, remarking that "we cannot have a dictator imposing censorship in the U.S."[36] The president's critical remarks were reportedly poorly received by Sony employees and dealt a blow to employee morale.[37]

Thus, although Sony Pictures is not a defense contractor, or indeed of any real national security significance, the North Korean attack against it gives us some idea of the potential damage that a wartime cyberattack against a private enterprise might cause. Severe operational disruption, leaks of confidential data, corporate embarrassment, and reduced employee morale are all to be expected if a private enterprise is the victim of a successful cyberattack. If a wartime cyberattack were to cause similar disruption at a defense firm or another similarly critical private enterprise, it could seriously impact the affected nation's war effort by disrupting production of war material and exposing state secrets. Thus, citizens and governments should expect that not only government-run services to come under attack, but also that private companies will be priority targets of wartime cyberattack.

---

https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

Andrea Peterson, "The Sony Pictures Hack, Explained," Washington Post, December 18, 2014, sec. The Switch, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

[34] Ibid

Kello, "The Quest for Cyber Theory", 55

[35] Cieply and Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm,"

[36] Ibid

[37] Ibid

Defenses and Looking Forward

The most straight-forward step governments could take to prevent massive disruption that could be caused by wartime cyberattacks is to take steps to harden the vulnerable industrial control systems and keep the desktop operating systems on which services depend fully patched. Though these steps are logical, hardening industrial control systems is a significant technical undertaking. I am not optimistic that governments can be relied on to keep their desktop operating systems up-to-date, as the problem of unpatched systems within a health service should never have occurred in the first place. Hence, infrastructure and services will remain easy targets for wartime cyberattack for the foreseeable future.

But although adhering to basic computer security best practices may mitigate some cyberattacks, such precautions will not provide blanket protection against cyberattacks. Undiscovered and unpublicized exploits will likely always exist in commercial software and if states are willing to expend significant resources to develop sophisticated malware such as Stuxnet, no computer system is ever going to be completely resistant to cyberattack should war break out.

More drastic defenses are also difficult, undesirable, or unfeasible. Porche, Sollinger, and McKay point out that people often discuss defending U.S. cyberspace in the same terms as defending a physical space and that such thinking does not translate well to cyberspace.[38] Further, building the cyberspace equivalent of a wall to attain the kind of total network isolation that would render a nation proof against external cyberattack is difficult to achieve and not always desirable. Porche, Sollinger, and McKay illustrate their point that American cyberspace depends on servers all over the world by pointing to "the near ubiquitous BlackBerrys carried by government officials and private-sector employees" which depend on Canadian severs.[39] Although BlackBerrys are not as significant in the public or private sectors as they

[38] Porche, Sollinger, McKay "A Cyberworm That Knows No Boundaries", 2
[39] Ibid

once were, the wider claim that it is difficult and perhaps undesirable to "[fence] off' an internet-dependent nation's cyberspace from the internet as a whole is sound.[40]

Thus, as commercial software will almost certainly be vulnerable in perpetuity, states have already developed sophisticated cyber-weapons and taking drastic measures to cut off an Internet-dependent nation from the wider Internet is difficult and undesirable, an iron-clad defense against wartime cyberattacks is probably impossible for an internet-dependent nation to achieve. Therefore, in a future war between Internet-dependent nations, cyberattacks will occur, no matter how well the belligerents prepare their defenses. Thus, policymakers should also pay careful attention to preparations for recovering from successful cyberattacks in addition to ensuring that government services and private companies adhere to security best practices.

Conclusions

In short, cyberattacks are an inevitable in a future war between Internet-dependent nations as attacks carried out in peacetime have demonstrated the feasibility and efficacy of as-yet-hypothetical wartime cyberattacks. From damaging or disabling critical infrastructure to disrupting the operations of private companies, the cyberattacks examined in this paper have shown that cyberattacks could be an effective means of accomplishing many strategic objectives in a time of war.

Furthermore, it is impossible for an Internet-dependent nation to make itself impervious to cyberattacks. While some attacks cyberattacks can easily be defended against, the NHS could have avoided damage from WannaCry if they had kept their Windows installations up-to-date for instance, it is practically impossible for a nation to defend against all possible cyberattacks.[41] Undiscovered vulnerabilities will always exist in commercial software – for example, at the time of this writing, a severe

[40] Ibid
[41] Hall, "NHS Could Have 'Fended Off' WannaCry by Taking 'Simple Steps' – Report,"

vulnerability in macOS that allowed an attacker to effortlessly gain root access to a system had recently been publicized – so it is impossible to guarantee that commercial operating systems and applications are perfectly secure.[42] The existence of sophisticated cyberweapons like Stuxnet indicates that states are willing to go to extraordinary lengths to develop and deploy sophisticated cyberweapons that are effective against hardened systems. Thus, defending the entirety of a nation's infrastructure against cyberattacks from capable and determined attackers is practically impossible.

Given the certainty that cyberattacks will play a role in future wars and the impossibility of defending against wartime cyberattacks is impossible, governments and corporations should instead focus on mitigating the most obvious threats via following security best practices and managing the fallout from successful wartime cyberattacks when they occur. In a time of war, successfully managing the destruction wrought by cyberattacks might be the best anyone can hope for.

[42] Dan Goodin, "macOS Bug Lets You Log in as Admin with No Password Required," Ars Technica, November 28, 2017, https://arstechnica.com/information-technology/2017/11/macos-bug-lets-you-log-in-as-admin-with-no-password-required/