The Mouse Clicks of August: Hybrid Warfare, Nation-State Actors, and the Future of Cybersecurity

Jeff Dougherty

Although hacking has been part of espionage since at least 1989[1], nation-state sponsored attacks have grown dramatically throughout the past decade[2,3,4]. Nation-state sponsored groups are particularly worrisome to security professionals because they often operate as Advanced Persistent Threats (APTs)[5], a "slow burn" type of cyberattack many security experts consider the most dangerous for enterprises- or governments- with highly sensitive information to protect[6,7,8]. However, a deeper look at the pattern of these attacks in recent years reveals a still more worrying trend. In the last decade, nation-state backed hacker groups have shifted away from pure information gathering and towards using cyberspace as a domain for a new kind of conflict called hybrid warfare.

Hybrid warfare is difficult to define, and some thinkers even doubt the utility of the concept[9]. However, others have defined it as aggressive actions designed to exploit international law by deliberately falling short of the common definition of aggression that permits a response against a nation-state[10]. Hybrid warfare is a type of asymmetric warfare, in which a weaker opponent seeks to defeat a stronger one by indirect means without having to engage their main military forces.[11] The concept's supporters frequently cite the civil war in Eastern Ukraine, where suspiciously well trained and equipped "pro-Russian separatists" have given Moscow effective control over large chunks of territory without a conventional invasion that could trigger the NATO treaty[12]. Also commonly cited are "salami slicing" tactics used by China to slowly establish a position of effective dominance over disputed islands in the South China Sea,[13] including use of its fishing fleet to establish territorial claims.

Cyberspace is an especially rich field for hybrid warfare because the global and anonymous nature of the Internet makes it very difficult to prove a particular operation was state-sponsored. For example, a

group codenamed APT28 has been identified as a Russian government operation based on their use of Russian-language programming tools, the fact that they keep 9-5 hours on Moscow time and observe Russian holidays, and the overlap between their operations and Russian interests[14]. Suggestive, but hardly the sort of thing you can take to the United Nations. Online, hybrid warfare can involve a variety of methods, including denial-of-service (DoS) attacks against a target's communications, obtaining and leaking embarrassing information about the target, or interfering with a target's critical infrastructure.

Most state-sponsored hacks discussed in the open security press originate from a relative handful of nations: China, Russia, Iran, North Korea, Israel, and the United States[15,16,17]. An examination of recent actions by hackers affiliated with those countries reveals an increasing pattern of offensive action.

Of the nations listed, it is Russia that has taken by far the largest steps into online hybrid warfare. Beginning with a massive DoS attack against Estonia in 2007[18], Russia has used cyberwarfare as a major component of its operations in Georgia[19], the Ukraine[20], and Syria[21]. The scope of attacks has also widened with time. The 2008 Georgia attacks included more DoS against communications infrastructure, attempts to glean military intelligence from online sources, and propaganda defacement of websites. Attacks against Ukraine in 2015 repeated these tactics, but also saw Russian hackers shut down large portions of the Ukrainian power grid. 2015 also saw Russia shut down German government websites and a steel mill around the time of talks with the Ukrainian Prime Minister.[22] The next year brought the publicized attempts to influence the US Presidential election by selectively releasing illegally obtained documents about the Hillary Clinton campaign. Taken as a whole, it is clear that Russia does not simply regard cyberattacks as an information gathering tool, but as weapons to be used offensively in support of Moscow's geopolitical aims.

Similar patterns have appeared on a smaller scale from the other nations on the list. Most famously, the US and Israeli-developed Stuxnet worm was released onto the Internet in 2009, replicating itself until it reached the computer controllers for Iran's uranium enrichment centrifuges. Once there, it caused the centrifuges to overspeed while loaded with corrosive uranium gas, damaging them and seriously delaying the Iranian nuclear program[23]. The same US-Israeli effort led to the creation of a piece of network reconnaissance malware called Flame, which provided information Israel later used to launch a unilateral attack on the Iranian oil industry in 2012 with a program called Wiper[24]. Other information about these countries' cyberwar programs is hard to come by, but the April 2017 leaks from a group calling themselves ShadowBrokers revealed that both the American CIA and NSA have been actively developing their own ecosystem of tools and exploits[25].

The Stuxnet and Wiper incidents seem to have spurred Iran to create its own hacking program. The year after the attacks, Iran attacked banks and a dam in the United States[26] as well as oil company systems in Saudi Arabia[27,28] using malware descended from Israel's Wiper. Iranian hackers have also been implicated in a 2015 blackout that affected 40 million people in Turkey[29]. It is significant that the Iranian hacking program appears to be associated with the country's Revolutionary Guard Corps, or Pasdaran. Ever since the Iran-Iraq War of the 1980s, the Pasdaran has been the main Iranian force involved in all types of asymmetric warfare. The placement of Iran's hacking groups under their control may well indicate that the Iranian government views them primarily as weapons of war.

North Korea's cyber program is best known in the West for its 2014 hack of Sony Pictures[30], but has also been implicated in several other operations. These include the DarkSeoul attacks against South Korean infrastructure[31] and spreading malware to create botnets for denial-of-service attacks[32]. Many experts also believe North Korea is attempting to use its cyber program to finance its regime in the face of international sanctions- North Korean hacking groups have been tied to the WannaCry ransomware

attack, the theft of $80 million from a bank in Bangladesh[33], and may also be targeting the crypto-currency Bitcoin[34].

At first glance, China's hacking efforts may seem the odd man out in this group. China has taken little overt action online, although it is a prolific practitioner of cyber espionage. Its' operations have not been confined to traditional government and military targets, frequently targeting private companies to steal intellectual property that may improve the competitiveness of China's state-run businesses.[35,36]. However, it is known that China's military planning documents anticipate intensive network operations in the event of a war, and at least one analyst has argued that China's current actions are preparing it for exactly that[37]. China appears to think that the US needs the Internet more than they do, and that an exchange that leaves both sides' networks severely degraded is a net win for them. They are probably right.

If these trends are alarming, there is little reason to think they will not continue. There have been some promising signs. The indictment of five Chinese army officers for hacking American servers led to an agreement between President Obama and Chinese President Xi Jinping under which China would reduce its attacks against American companies[38], and attacks did seem to decrease in the wake of the agreement[39]. However, a similar indictment of seven Pasdaran-affiliated Iranian hackers in 2013 has failed to yield similar results[40], and efforts to confront Russia over its ever more brazen attacks have also stalled in the face of official stonewalling. More broadly, a number of analysts[41] have noted that the West has largely failed in its attempts to address hybrid warfare incidents that fall short of the clear aggression required to form international consensus. Given the nature of the Internet, cyberattacks are likely to remain one of the most difficult of all incidents to provably attribute to a government. The relative newness of the Internet also means that international law on acceptable online behavior between nations is still very much unset. Absent strong new norms of what is and is not acceptable

between nation-states in peacetime, it is likely that both the number and severity of these cyberattacks will continue to escalate.

What does this mean for cybersecurity professionals? The first and most important lesson we can draw is that in a cyberwar, everybody is potentially on the front lines. Cyberattacks from all nations have made little distinction between government-owned and private systems, instead choosing to strike wherever necessary to accomplish their goals. Private companies, especially those in key infrastructure settings, need to be prepared to compete with teams of government-sponsored hackers from around the world. Second, to whatever extent this is unrealistic, there must be closer cooperation between the public and private sectors. The government may need to provide assistance with network hardening, penetration testing, and threat intelligence, not to safeguard private profit but to preserve critical national infrastructure. This assistance should be tied to a set of legally enforceable standards to make sure those trusted with critical information are taking adequate precautions to safeguard it. Finally, on the policy level, high-level leaders should work to create new standards for what is and is not acceptable in terms of hacking between nations at peace. This will not be an easy task, requiring both a willingness to engage with nations who show openness to the new standards and to take a firm line with those who do not. But if we fail to do so, the cyber realm we trust with more and more of our data may become a new theater of war. And if that happens, everyone and everything on the global Internet could become collateral damage.

1 Stoll, Clifford. The Cuckoo's Egg. Doubleday, 1989. The East German hacker responsible for that incident was operating on behalf of the Soviet KGB.
2 McGuiness, Damien. "How a cyber attack transformed Estonia." BBC News, http://www.bbc.com/news/39655415 Accessed 10/2/2017
3 Rubenstein, Dana. "Nation State Cyber Espionage and its Impacts." Washington University in St. Louis. http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. Accessed 10/2/17
4 For a longer listing, see the Center for Strategic and International Studies' "Significant Cyber Incidents Since 2006" report, available for download at https://csis-prod.s3.amazonaws.com/s3fs-public/160824_Significant_Cyber_Events_List.pdf
5 "A Survey of Nation-State Sponsored Hackers," published by DarkOwl Security. https://www.darkowl.com/blog/2017/a-survey-of-nation-state-sponsored-hackers. Accessed 10/2/17
6 Soto, Carlos. "Advanced Persistent Threats (APT) 101." Tom's ITPro. http://www.tomsitpro.com/articles/advanced-persistent-threats-apt-101,2-526.html. Accessed 10/2/17
7 "The Danger of Advanced Persistent Threats." Published in BizTech Magazine, attr to staff. https://biztechmagazine.com/article/2016/05/danger-advanced-persistent-threats. Accessed 10/2/17
8 "Advanced Persistent Threats: A Symantec Perspective." Symantec White Papers. https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf. Accessed 10/2/17
9 Paul, Christopher. "Confessions of a Hybrid Warfare Skeptic." Small Wars Journal, March 3, 2016. http://smallwarsjournal.com/printpdf/40741. Accessed 10/2/17
10 For discussions of this issue, see Stowell, Joshua, "What Is Hybrid Warfare?", Global Security Review. https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/ and Sarl, Aurel, "Legal Aspects of Hybrid Warfare", Lawfare Blog. https://www.lawfareblog.com/legal-aspects-hybrid-warfare, both accessed 10/2/17
11 This is a simplification of a complex concept, but is the definition that will be used for this paper. For a good discussion of asymmetric war and its place in the landscape of military strategy see Daley, LTC Dan N, "Asymmetric Warfare: The Only Thing New Is the Tactics", a seminar paper from the US National War College available at http://www.dtic.mil/dtic/tr/fulltext/u2/a433588.pdf
12 Chivvis, Christopher S. "Understanding Russian Hybrid Warfare and What Can Be Done About It." Testimony presented to the House Armed Services Committee on March 22, 2017 on behalf of RAND Corporation. Available at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.
13 Shearer, Andrew. "The Evolution of Hybrid Warfare and Key Challenges," Statement to the House Armed Services Committee on March 22, 2017. Available at http://docs.house.gov/meetings/AS/AS00/20170322/105746/HHRG-115-AS00-Wstate-ShearerA-20170322.pdf
14 "APT28: A Window into Russia's Cyber-Espionage Operations?" Report published by the FireEye Corporation, 2014. Available at https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
15 A Survey of Nation-State Sponsored Hackers," published by DarkOwl Security. https://www.darkowl.com/blog/2017/a-survey-of-nation-state-sponsored-hackers. Accessed 10/2/17
16 Walls, Mike. "Nation-State Cyberthreats: Why They Hack." DarkReading. https://www.darkreading.com/informationweek-home/nation-state-cyberthreats-why-they-hack-/a/d-id/1318522. Accessed 10/2/17
17 This datum should be treated with a certain degree of caution. The open security press itself is largely a Western phenomenon- of the 500 top cybersecurity firms, 370 are American and a further 76 are based in Canada, Europe, or Australia. Thus, cyberattacks not targeted against these countries are probably less likely to be discussed in the open press. Source: analysis of data provided by Cybersecurity Ventures, available at https://cybersecurityventures.com/cybersecurity-500-list/, accessed 10/2/17
18 Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for US National Security." International Affairs Review, published by George Washington University. http://www.iar-gwu.org/node/65. Accessed 10/2/17.
19 Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal, January 6, 2011, available at http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
20 Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." Wired.com, 6/20/17. Available at https://www.wired.com/story/russian-hackers-attack-ukraine/, accessed 10/2/17
21 "Behind the Syrian Conflict's Digital Front Lines," Threat Intelligence Report by FireEye Corporation. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf, accessed 10/2/17
22 Walls, Mike. "Why Russia Hacks." DarkReading. https://www.darkreading.com/risk/why-russia-hacks/a/d-id/1318733. Accessed 10/2/17

23 Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf. Accessed 10/2/17
24 Nakashima, Ellen, Greg Miller and Julie Tate. "US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. Accessed 10/2/17
25 Goodin, Dan. "NSA-leaking Shadow Brokers just dumped its most damaging release yet." Ars Technica, https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/. Accessed 10/2/17
26 Perez, Evan and Shimon Prokupecz. "US charges Iranians for cyberattacks on banks, dam." CNN.com. http://www.cnn.com/2016/03/23/politics/iran-hackers-cyber-new-york-dam/. Accessed 10/2/17
27 Zetter, Kim. "Wiper Malware That Hit Iran Left Possible Clues of Its Origins." Wired.com https://www.wired.com/2012/08/wiper-possible-origins/. Accessed 10/2/17
28 Greenberg, Andy. "New Group of Iranian Hackers Linked to Destructive Malware." Wired.com. https://www.wired.com/story/iran-hackers-apt33/. Accessed 10/2/17
29 Paganini, Pierluigi. "Iran accused of the blackout that paralyzed the Turkey" (sic). Securityaffairs.co http://securityaffairs.co/wordpress/36536/cyber-warfare-2/iran-accused-blackout-turkey.html. Accessed 10/2/17
30 Peterson, Andrea. "The Sony Pictures hack, explained." The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. Accessed 10/2/17
31 "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War." Symantec.com. https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war, accessed 10/2/17
32 "Revisiting Nation State Threat Actors- North Korea (DPRK). Published by DarkOwl Security. https://www.owlcyber.com/blog/2017/revisiting-nation-state-threat-actors-north-korea-dprk. Accessed 10/2/17
33 Finkle, Jim. "Cyber security firm: more evidence North Korea linked to Bangladesh heist. Reuters. http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4. Accessed 10/2/17
34 McNamara, Luke. "Why Is North Korea So Interested in Bitcoin?" FireEye Security Blog. https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html. Accessed 10/2/17
35 Walls, Mike. "Nation-State Cyberthreats: Why They Hack." DarkReading. https://www.darkreading.com/informationweek-home/nation-state-cyberthreats-why-they-hack-/a/d-id/1318522. Accessed 10/2/17
36 US Department of Justice press release. "US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage." https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. Accessed 10/2/17
37 McReynolds, Joe. "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy." China Brief, Vol. 15 Issue 8, available at https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/
38 Harold, Scott Warren. "The US-China Cyber Agreement: A Good First Step." Rand Corporation. https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html. Accessed 10/2/17
39 "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," Published by FireEye Corporation, June 2016. Available at https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, accessed 10/2/17
40 US Department of Justice Press Release. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against US Financial Sector. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged. Accessed 10/2/17
41 See Radin, Andrew, "Hybrid Warfare in the Baltics: Threats and Potential Responses," RAND Corporation 2017, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf, and Schadlow, Nadia, "The Problem With Hybrid Warfare", *War on the Rocks* April 2, 2015