15

Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace

Anne-Marie Buzatu[*]

1 INTRODUCTION

Their attacks do not typically result in gruesome pictures nor grab the international headlines in the same way as their physical, armed counterparts, but they may be just as deadly or even more dangerous: Advanced Persistent Threat Groups (APTs) are on the rise and changing the very character of modern international conflict today, with yet to be fully appreciated consequences. Operating in obscurity behind screens where they can largely remain anonymous, and called such fanciful names as "Red Apollo" or "Cosy Bear," little is known for certain about who is manning these groups or to whom their allegiances ultimately lie.[1] Rather, analysts try to piece together this information by identifying patterns in cyberattacks, seeing whether the targets of the attack align with the interests of certain states, as well as finding the occasional digital traces that the groups or their members may have left online. What these groups lack in physical bravado they more than make up for in real-world damaging consequences. The COVID-19 pandemic has only served to further accelerate the global dependence upon technologies, providing APTs more opportunities to wreak international havoc and destabilization.

While not officially acknowledged by states, APTs are allegedly run by or sponsored by states to gain unauthorized access to computer systems of governments or companies, where they remain undetected for an extended period of time and gather information, including sensitive information about defense capabilities and critical infrastructure control systems. Recent times have seen the emergence of nonstate sponsored APT groups carrying out large-scale intrusions into

[*] ICT4Peace is an independent foundation that fosters political discussion and common action to support international and human security in cyberspace. To this end, it researches, identifies, and raises awareness about emerging technology challenges, makes policy recommendations, and delivers capacity-building programs.

[1] More information about the forms APT attacks take place can be found here: https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

https://doi.org/10.1017/9781108954341.015 Published online by Cambridge University Press

government or commercial network systems, sometimes for criminal/financial gain.[2,3]

The "Solarwinds" attack, discovered in December 2020, vividly illustrates both the damage and the uncertainty these kinds of attacks can cause. Analysts said the attack resembled those in the past, thought to have been carried out by Russian-based APTs "Cosy Bear," also known as "APT29,"[4] but Russia has denied any involvement,[5] and the identity of the attack's author is not known for certain, although it seems fairly sure that it is another government.[6] However, apart from the inability to reliably attribute the attack, the extent of the attack itself, as well as the potential security risks it engendered, are also uncertain. What is known is that US agencies, important for the nation's security, were compromised, including the US departments of Homeland Security, State, Commerce and Treasury, the National Institutes of Health, as well as nuclear programs run by the US Department of Energy and the National Nuclear Security Administration.[7] The lack of clarity regarding the information that was stolen, as well as whether critical systems were compromised, has generated a lot of anxiety about the security of US defense systems, with some experts calling for the United States to strike back at Russia.[8] Clearly, APT attacks are turning the traditional international security and peace paradigm on its head, with commensurate risks to our collective safety and security.

2 KINDS OF ATTACKS

APT attacks generally fall into the following categories:

2.1 *Espionage*

APTs infiltrate computer systems and networks and gather information. Targets typically are governments, companies, or other organizations.

For example, an APT group that seemed to be based in China have reportedly targeted South East Asian government machines since at least November 2018, infecting over 200 government machines and even installing backdoors so that they could easily access machines going forward.[9] Other reports claim that

[2] See, Maloney, Sarah, "What is an Advanced Persistent Threat (APT)," last accessed November 29, 2020.
[3] "Why nation-state cyberattacks must be top of mind for CISOs," TechTarget Network, last accessed November 29, 2020.
[4] "Microsoft Discovers a Second Hacking Team Exploiting SolarWinds Orion Software," *CPO Magazine*, last accessed February 16, 2021.
[5] "SolarWinds software used in multiple hacking attacks: What you need to know," ZDNet, last accessed February 16, 2021.
[6] Ibid.
[7] Ibid.
[8] "Cybersecurity experts say US needs to strike back after Solarwinds hack," CBS News 60 Minutes Overtime, last accessed February 16, 2021.
[9] See, for example, "Dissecting a Chinese APT Targeting South Eastern Asian Government Institutions," Bitdefender Draco Team Whitepaper, last accessed November 29, 2020.

https://doi.org/10.1017/9781108954341.015 Published online by Cambridge University Press

three state-sponsored APTs operating from Russia and North Korea attempted to break into the computer systems of at least seven prominent companies involved in COVID-19 vaccine research and treatment in order to steal sensitive information.[10]

2.2 *Critical Infrastructure Attacks*

The industrial control systems (ICS) that operate and control critical infrastructure systems have been targeted by APTs, which use sophisticated attacks to deactivate, take over control, or destroy them. These include the ICSs of energy grids, water supply systems, electricity production plants, nuclear installations, and banking and telecommunications systems.

One of the earliest of these kinds of attacks that garnered international attention was the 2010 Stuxnet worm that targeted supervisory control and data acquisition (SCADA) systems, which operate the systems that control large-scale machinery and industrial processes, including energy grids and nuclear installations. In this instance, the Stuxnet worm reportedly ruined nearly one-fifth of Iran's nuclear centrifuges by infecting over 200,000 computers and physically damaging approximately 1,000 machines.[11] While no state officially took responsibility for the attacks, analysts largely believe that groups associated with the United States and Israel were behind them.[12]

In the time since the Stuxnet attack, attacks on important and critical infrastructure control systems have continued and increased. For example, in April of 2020, the command and control systems of Israeli water supply systems were reportedly breached by an APT associated with Iran. However, the Israeli government did not disclose any further information regarding the impact of the attack.[13] Additionally, in February 2021, a water treatment plant in the US state of Florida was attacked by a hacker who managed to break into the water treatment control system and increase the levels of lye in the water from 100 parts per million to 11,100 parts per million, which would have made anyone who drank the water very sick. Fortunately, a water plant operator happened to be looking at the ICS screen and witnessed in real time the changes to the levels, correcting them before the changes contaminated the water. However, the computer security systems of the water plant's ICS were not robust enough in themselves to prevent the damage, meaning that if the operator had not happened to be looking at those levels at that particular moment, the water would have been contaminated.[14]

[10] "See Microsoft says three APTs have Targeted Seven COVID-19 Vaccine Makers," available online at: www.zdnet.com/article/microsoft-says-three-apts-have-targeted-seven-covid-19-vaccine-makers/.

[11] "Sheep dip your removable storage devices to reduce the threat of cyber-attacks," Solutions, last retrieved November 29, 2020.

[12] "Stuxnet was work of U.S. and Israeli experts, officials say," *Washington Post*, last accessed 16.02.2021.

[13] Goud, Naveen, "Israel Water Supply Authority hit by Cyber Attack," Cybersecurity Insiders, last accessed November 29, 2020.

[14] "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," *New York Times*, last accessed February 16, 2021.

https://doi.org/10.1017/9781108954341.015 Published online by Cambridge University Press

2.3 *Interference in the Electoral Processes*

APTs are also putting their skills to work at interfering with and undermining national electoral processes.

For example, the US government Cybersecurity and Infrastructure Security Agency (CISA) issued an alert in October 2020, saying that Iranian APTs were creating fictitious websites as well as posting "fake news" to legitimate media platforms in order to undermine public confidence in election systems, as well as to further divide public opinion.[15] US intelligence agencies also reported that Russia interfered in the 2016 US elections, under the direct orders of Russian President Vladimir Putin who, they say, used "troll farms" to create thousands of fake social media accounts to influence popular opinion.[16]

2.4 *Information System Attacks*

Another kind of attack aims to bring down the networks and computer systems so that they are no longer available online.

For example, an APT allegedly associated with North Korea, known as the "Lazarus Group," reportedly took down the Sony Corporation website in retaliation for its release of the film The Interview, a controversial comedy that portrayed US journalists recruited by the US government to assassinate North Korea leader Kim Jong-Un.[17]

2.5 *Ransomware Attacks*

Recently, there has been a sharp increase in ransomware attacks, or attacks in which an organization's data has been stolen or computer systems rendered unavailable, with attackers demanding they be paid a ransom to return data or restore access. In 2020, these kinds of attacks increased by an estimated 319 percent, with perpetrators bringing in at least $350 million (USD).[18]

The above-mentioned "Lazarus Group" APT has also been blamed for one of the most significant ransomware attacks, known as "Wannacry," which was released in May 2017 and infected around 200,000 computers located in 150 different countries.

[15] "Iranian Advance Persistent Threat Actors Threaten Election-Related Systems," US Cybersecurity & Infrastructure Security Agency Alert (AA20–296B), published October 22, 2020, last accessed November 29, 2020.

[16] Ross Brian, Schwartz Rhonda, Meek James Gordon, "Officials: Master Spy Vladimir Putin Now Directly Linked to US Hacking," ABC News, last accessed November 29, 2020.

[17] Heller, Michael, "Lazarus Group hacker charged in WannaCry," Sony attacks, TechTarget Network, last accessed November 29, 2020.

[18] "Ransomware gangs made at least $350 million in 2020," ZD Net, published February 2, 2021, last accessed February 16, 2021.

Of particular note, the National Health Service (NHS) hospitals in England and Scotland were hit, requiring the NHS to cancel many noncritical procedures and treatments.[19]

In September 2020, in what was possibly the first account of a ransomware attack on a hospital resulted in the death of a patient in Dusseldorf, Germany. Having fallen victim to a ransomware attack, the hospital had to reroute the patient's ambulance to another hospital, during which the patient died. Of note, the attacked hospital was not the intended victim of the attack, as the ransom note was addressed to a nearby university. The attackers stopped the attack once authorities informed them that it had shut down a hospital, however, this came too late to save the victim.[20]

In addition to the serious, even life or death consequences for health, both of these attacks also illustrate another difficulty about cyberattacks; that is, their often indiscriminate nature, infecting systems and devices across the Internet where they find vulnerabilities, and not just the intended target(s).

3 "CYBER HYBRID WARFARE": AN EMERGING THREAT TO CYBER PEACE

The activities and cyberattacks carried out by APTs are changing the character of international conflict today. In the words of Australia's Defense Minister, Linda Reynolds:

> [w]hat is clear now, is that the character of warfare is changing, with more options for pursuing strategic ends just below the threshold of traditional armed conflict – what some experts like to call "grey-zone tactics" or "hybrid warfare."[21]

More worryingly, the nature of these "grey-zone tactics" by and large slip through the cracks of our international legal frameworks, most of which were constructed around underlying assumptions that attacks would be physical or kinetic, and that states had effective territorial control to uphold their international obligations and protect those within their jurisdictions. By contrast, the "cyber hybrid warfare" paradigm thrives in an environment where "cyberattacks" often do not fulfill the requirements of international conventions, in which states do not acknowledge their responsibilities for such acts, and in which private actors can act on behalf of – or in the place of – international legal personalities.

In this new paradigm, all stakeholders can be authors of attacks as well as the victims – oftentimes both state and nonstate actors are injured by the same attacks

[19] "Cyber-attack: Europol says it was unprecedented in scale," BBC News, published 13 May 2017, last accessed November 29, 2020.

[20] Wetsman, Nicole, "Woman dies during a ransomware attack on a German hospital," The Verge, published September 17, 2020, last accessed November 29, 2020.

[21] Dowse, Andrew and Bachmann, Sascha-Dominik, "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?" The Conversation, published June 17, 2019, last accessed November 29, 2020.

online – and effective defense against such attacks may more likely come from the private sector instead of public security forces. If we are to adapt the international legal order to one that supports cyber peace, this calls for new thinking and innovative approaches. While the scope of this essay is not such as to go in-depth into conceiving such a paradigm, as this has already been done throughout this volume, in constructing this new framework, from our perspective, the following elements should be considered or reconceived.

3.1 *The Adaptation of International Legal Obligations and Norms to the Cyber Frontier*

While it is generally accepted that "international law applies online as well as offline," what is not always clear is what this means in practice within the interconnected, transborder environment of cyberspace. Furthermore, as states have implemented their international law obligations to reflect national cultural contexts and values, how do we reconcile these often different and sometimes incompatible state-specific standards within an interconnected, largely borderless cyberspace?

3.2 *The Notion of "Effective Control"*

Furthermore, what actor has the ability to effectively control online activities? Is it the company who owns an undersea cable that forms part of the Internet's backbone? Is it the company that owns the computer servers and/or the state in which those same servers are located? Is it the APT that has the knowledge to infiltrate and even control state and commercial computer systems? When reconsidering the notion of "effective control," we should look carefully at which actors have the know-how/capability to effectively stop or prevent the kinds of behaviors online that undermine cyber stability and cyber peace. This issue is part and parcel of creating an effective regime to regulate state-sponsored cyber aggression.

3.3 *Responsibility and Accountability v. Protection*

Finally, as actors have the ability to carry out activities anonymously, private actors sometimes pack more cyber power than states, and states do not publicly acknowledge their involvement in many attacks, how do we craft a system in which there is effective responsibility and accountability for online attacks? Perhaps this question should be turned around and be considered from a human security point of view as the CyberPeace Institute suggests,[22] asking how can we best protect the human rights and safety of individual users/netizens online?

[22] "CyberPeace: From Human Experience to Human Responsibility," Medium, last accessed February 16, 2021.

https://doi.org/10.1017/9781108954341.015 Published online by Cambridge University Press

Recent initiatives offer some promising avenues to pursue. For example, the Office of the High Commissioner on Human Rights (OHCHR) B-Tech project, which aims to apply the UN Guiding Principles on Business and Human Rights to the ICT sector, is looking at how to create a "smart mix of measures" by exploring regulatory and policy responses to human rights challenges linked to new technologies.[23] UN Secretary-General António Guterres launched a High-Level Panel on Digital Cooperation, bringing together actors from public and private sectors to advance discussions on improving cooperation in cyber governance, which resulted in the "UN Secretary-General's Roadmap on Digital Cooperation."[24] Both France's Paris Call for Trust and Security in Cyberspace[25] and New Zealand's Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online[26] call on both governments and the ICT commercial sector to join forces in combatting malicious attacks online. Microsoft has been very active in the cyber governance space, launching a number of different initiatives, such as the Cyber Tech Accord,[27] to advance multistakeholder discussions at the international level. My organization ICT4Peace, a CSO, has called on governments to publicly commit to refrain from cyberattacking critical infrastructures[28] – which in principle should extend to the APTs they are affiliated with – and called for the creation of a state peer review mechanism on the order of the Human Rights Council's Universal Periodic Review to provide some oversight and accountability for states' actions online.[29]

All of these initiatives recognize the piecemeal, polycentric, multistakeholder-driven nature of cyberspace, and further that it will take joint efforts and concerted collaborative action toward a goal that is in all of our best interests: A safe and peaceful cyberspace in which all stakeholders can thrive and in which state and human security go forward hand-in-hand.

[23] "Business and Human Rights Technology Project ('B-Tech Project'): Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies," last accessed November 30, 2020.
[24] For more information, see www.un.org/en/digital-cooperation-panel/, last accessed November 30, 2020.
[25] For more information, see pariscall.international/en/, last accessed November 30, 2020.
[26] For more information, see www.christchurchcall.com, last accessed November 30, 2020.
[27] For more information, see cybertechaccord.org, last accessed November 30, 2020.
[28] "Call to Governments to refrain from carrying out offensive cyber operations and cyberattacks against critical infrastructure."
[29] Cyber Peer Review Mechanism.