Cyberruse at the Cybergates

Technology, People and Processes

In 1587, Spain was at war with England. Under King Philip of Spain, the Spanish Empire built an armada of 130 large battleships, all waiting in the bay of Cadiz, Spain, ready to invade England.[1] Cadiz was fortified. A series of sandbanks, lookout stations, and a large battery of shore guns defended more than 100 Spanish and French ships. They served as firewalls and intrusion detection systems (IDS), all trained to spot predefined modes of incursion.

But Britain, led by Sir Francis Drake, the famous privateer (a private party conducting war on behalf of a country for money [ransom or loot] and fame) under Queen Elizabeth I, intended to fool the Spanish defense at Cadiz with a *ruse de guerre,* or deception of war.

Drake's 24 ships, 80 percent of them merchant vessels, were technically inferior to the more numerous and battle-ready Spanish and French warships. But Drake knew that war is more than technical or numerical superiorities. He realized that weaknesses lie in process inefficiencies and human fallibility, and on the evening of 29 April 1587, a time of day when it was customary for Spanish people to relax, Drake leveraged process inefficiencies by entering the bay at dusk. Drake also took advantage of human fallibility. As his ships entered the bay, he ordered that all English flags be furled to confuse the Spanish lookouts, leaving them unsure of whether the incoming ships were friend or foe. By the time the Spanish realized the ruse, Drake's fire ships had ignited multiple opposition ships. Between 27 to 37 warships of the Spanish Armada were destroyed in 36 hours.[2]

Drake's tactics offer clues about the evolving nature of cyberwarfare in modern times.

First, Drake was not a part of the regular British Navy, but a privateer. Cyberwarfare is rapidly being outsourced to state-sponsored, third-party privateers such as Darkside in Russia and Chengdu 404 in China.

Second, Drake's attack on the Bay of Cadiz did not rely on brute force but that of a ruse that leveraged the enemy's warfare conventions along with its human and procedural inefficiencies. Analogously, cyberprivateers do not practice brute-force attacks. Instead, they use cyberruses to fool the enemy and stealthily penetrate enemy defenses for ransom or disruption. Organizations across the world must be prepared for these kinds of attacks.

Privateers and Ruses in Cyberwarfare

Cyberwarfare is becoming a war of ruses for ransom or disruption. But cyberwarfare is not a widespread military exercise amassing armies, air forces and navies across geographical borders. Instead, cyberwarfare uses the same tenets of warfare—offense, defense and destruction—without any rules of engagement. With the rapid proliferation of the Internet, the Internet of Things (IoT) and mobile devices, occurrences of cyberwarfare are rapidly gaining ground. Cyberwarfare can be conducted from any remote global location by savvy operators armed with a few computer programs and a network connection. In cyberwar, enemies are faceless and fluid. Their anonymity, disguise, and speed of appearance and disappearance make them dangerous perpetrators prompting an urgent need to secure the cybergates.

Unlike cyberattacks, which are isolated incidents, cyberwarfare is a concerted and deliberate campaign sponsored by a nation-state. But, as England did with Sir Francis Drake, nation-states are

Pratim Datta, Ph.D.
Is a professor of global information systems, digital transformation and cybersecurity at Kent State University (Ohio, USA) and a senior research scientist at the University of Johannesburg (South Africa). Datta is an internationally ranked researcher with more than 70 journal articles and conference proceedings and multiple best paper nominations and awards. Before academia, Datta worked for IBM Global Business Services and PricewaterhouseCoopers (PwC). He consults with organizations on process reengineering, cybersecurity and digital transformation.

outsourcing their sponsorship to a new generation of privateers. However, the nation-state is gradually becoming a passive sponsor. Nation-states can provide cyberprivateers with supporting technological infrastructure and political asylum. Cyberprivateers, instead of practicing *ruse de guerre* on high seas and ports for loot and glory, can then scout the Internet to find useful and profitable targets and determine their vulnerabilities and data assets that can be looted (stolen), hijacked or disrupted for ransom or a show of force.

> "THE MAIN THREAT IS NO LONGER THE LOSS OF PHYSICAL TERRITORY, BUT THE ADVERSE EFFECTS OF RANSOM, SUBTERFUGE, SABOTAGE AND IMPAIRMENT, WHICH CAN HOLD A NATION-STATE HOSTAGE."

In cyberwarfare, malicious actors continuously search for digital and cyberphysical vulnerabilities and capitalize on those weaknesses to adversely affect a nation-state's economic and operational infrastructure.[3] But the function of cyberwarfare has changed. The main threat is no longer the loss of physical territory, but the adverse effects of ransom, subterfuge, sabotage and impairment, which can hold a nation-state hostage. The threat of cyberwarfare is severe, and it has motivated countries to build up their cyberwarfare arsenals, with a focus on defending against advanced persistent threats (APTs) that are sophisticated, continuous and destructive.

Attack Vectors and Attack Surfaces: The Ruse Ingredients in Cyberwarfare

The key to understanding cyberwarfare lies in understanding the attack vector and the attack surface. Attack vectors are deliberate modes of engagement meant to penetrate attack surfaces (e.g., enemy defenses and enemy territory). Choosing attack vectors and attack surfaces is also crucial in physical warfare. In 1781, George Washington's continental army in the United States, in conjunction with the French Army and Navy, (the attack vectors) chose to besiege Yorktown, Virginia, USA, (the attack surface) to defeat Lord Cornwallis and gain American independence in 1783.[4]

During the D-Day landings in Normandy, France, the pincer strikes both inland and on beachheads were the attack vectors, and Normandy was the attack surface. During Germany's 1939 invasion of Poland that marked the beginning of World War II, the Nazi blitzkrieg into Poland was the attack vector and Poland was the attack surface. As another example, imperial Japanese aircraft carriers served as attack vectors while assaulting Pearl Harbor in Honolulu, Hawaii, USA, in 1941.

Similar to Francis Drake's *ruse de guerre*, hackers often use ruses to obfuscate the attack vector and attack surfaces. As in the D-Day example, the allied forces created a ruse that pointed at Calais, France, as the invasion point. Germany's 1939 invasion of Poland was particularly successful because of Germany's ruse of negotiation talks with the United Kingdom and France. Consequently, the Nazi blitzkrieg into Poland caught the country off guard. Similarly, during the attack on Pearl Harbor, Japan conducted negotiations with the United States as a ruse, while setting up a surprise attack on the US Pacific Fleet.

Parallel to conventional warfare, cyberwarfare follows a *quid pro quo* between entities. While cyberwarfare attackers seek to create attack vector ruses to maximize their attack surfaces, cyberwarfare defenders proactively minimize their attack surfaces while deterring and detecting attack vectors.

When cyberattackers choose cyberwarfare attack vectors and attack surfaces, they commonly leverage process and human shortcomings rather than brute-force technological attacks.

Several examples can be used to show how seemingly weaker actors can cripple a more sophisticated technological foe by leveraging standard operating procedures (SOPs) and human shortcomings and taking advantage of the reactive "wait-and-see" attitudes that exist in place of proactively evolving operational cultures.

How Fancy Bear Sabotaged Ukrainian Artillery

Like Sir Francis Drake's privateering raid on Cadiz, Spain, during the 2014 Crimea operation, Russia's chief intelligence directorate (GRU) collaborated with Fancy Bear (APT28), a state-sponsored hacking outfit, to sabotage Ukrainian artillery.[5]

As part of the ruse, Fancy Bear used a remote-access command and control (C2) and Beacon malware as the attack vector to compromise Ukrainian artillery positions and destroy Ukrainian 122mm D-30 towed howitzer artillery.[6] Fancy Bear also developed X-agent, a malware implant based on an existing artillery-targeting program called *Попр-Д30.apk* (Android Application Package [APK]), for the ruse.

As a subterfuge, Fancy Bear distributed the malware via social media and online military forums, and the Ukrainian armed forces unwittingly downloaded the malware. The malware carried a C2 Beacon, a malicious payload that could remotely communicate from an infected Android device being used in the field, relaying artillery locations, battery strength and movements. The malware pinpointed Russian attacks on the Ukrainian artillery, resulting in a loss of 20 percent of the Ukrainian D-30 howitzers.

The SolarWinds' SUNBURST Hack: The Devil Is in the Process

The Ukrainian artillery malware cyberruse became a signature intrusion strategy for future cyberattacks. The strategy is simple and remains effective:

- Find a popular crowd-sourced platform where like-minded people share information and code snippets.
- Assume a credible *nom de plume* (an assumed name) to infiltrate the group.
- Find and capitalize on vulnerable processes or individuals to hijack or infiltrate.
- Access and infect the asset with trojan malware.
- Deliver the trojan or weaponized malware as an innocuous asset back in the crowd-sourced platform.
- Infiltrate, communicate and disrupt.

> "INSTEAD OF USING AN OVERWHELMING DENIAL-OF-SERVICE (DOS) SHOCK-AND-AWE ATTACK, THE SUNBURST HACK ACTORS CAPITALIZED ON ROUTINE, SUBOPTIMAL SOFTWARE SUPPLY CHAINS AND IT PROCESSES."

The 2020 SUNBURST SolarWinds' Orion server hack used a similar cyberruse strategy. The SUNBURST hack illustrates how a well-regarded infrastructure and security solution can fall prey to ruses that leverage routine processes in the software supply chain to deceive and compromise multiple targets.[7]

SolarWinds' Orion server was a popular IT performance management software operating across a worldwide array of banks, corporations and government agencies, including the US Department of Homeland Security (DHS) and the US Treasury. This made SolarWinds a valuable hacking target and gateway into multiple organizations. Also, the SolarWinds Orion infrastructure monitoring and management software advised clients to exclude its software from antivirus and end-point detection and response (EDR) monitoring to reduce Type I errors (e.g., false positives from detecting routine activities as threats). This allowed perpetrators to infiltrate the Orion gateway itself, dramatically increasing the attack surface with multiple lines of access, communication and control.

Instead of using an overwhelming denial-of-service (DoS) shock-and-awe attack, the SUNBURST hack actors capitalized on routine, suboptimal software supply chains and IT processes.

The SUNBURST cyberattack vector began by capitalizing on GitHub, a popular cloud-based software project repository used by enterprises to collaboratively develop and fix software, as its initial attack surface (subsequently migrating to the SolarWinds' Orion Servers as the attack surface) with SUNBURST malware as the attack vector. The SUNBURST SolarWinds attack vector was a trojan virus that leveraged a suboptimal SolarWinds Orion Server update process as the attack surface,

Enjoying this article?

- Read *Technology, People and Processes–Cybersecurity Fundamentals Certificate. www.isaca.org/credentialing/itca/cybersecurity-fundamentals*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*.

highlighting how attack vectors capitalize on weak points even in the most fastidious of fortifications.

The trojan malware, SUNBURST, operated like a spy, moving laterally and constantly changing positions and credentials within the network for two weeks to avoid raising any suspicions due to an out-of-the-ordinary, flaggable surge in network traffic communications. Only when a worthwhile target was discovered would a signal trigger the cleverly disguised malicious payload, that then would mimic mundane communications and move laterally across the system, infecting, sniffing and relaying.

Protecting the Cybergates: Technologies, Processes and People

George Santayana, a Stanford University (California, USA) professor and philosopher, said "Those who fail to learn from history are condemned to repeat it."[8] Such is the case with cybersecurity.

There is lingering myopia in many organizations that cybersecurity should be relegated to technology and, subsequently, the IT department. But cybersecurity is not a siloed activity; it is an organizational imperative. Treating cybersecurity merely as a technical fix is myopic.

Cyberruses are meant to prey on psychology and processes, not just technology. It is easy for cyberattackers to capitalize on process efficiencies, as they are often products of traditional routines and individual habits. Correspondingly, it is easy for cyberattackers to prey on human greed, fears and biases. Unsurprisingly, faulty processes and faulty habits become a wellspring for cyberruses.

Cyberattackers often would rather surreptitiously log into a system by assuming an identity than forcibly hack into a system and risk detection. Cyberattackers often begin their cyberruses in chatrooms and via social media, disguising themselves as legitimate actors. A spoofed communication can easily lure users into compromising their identities and downloading malware. The nonchalant attitude of employees with home computers running obsolete operating systems and compromised passwords can increase this risk.

Cybersecurity is not just about building technological fortifications but also changing the organizational culture. In cyberwarfare, cyberattackers rarely practice large-scale technological assaults. Instead, there has been a dramatic increase in cyberruses, highlighting the need to shift the cybersecurity mindset to pay more attention to organizational processes and people.

Relegating cybersecurity to merely a technological solution without reengineering business processes and training employees to be continuously vigilant opens cyberwarfare gates to malicious state-sponsored privateers and their ruses. Ruses have been the mainstay of war, meant to obfuscate technology and instead exploit operational processes and human psychology. Sir Francis Drake's Spanish raid exploited the Spanish armada's over-reliance on fortifications and SOPs to create a ruse. Fancy Bear's Ukrainian artillery decimation relied on human and process deficiencies concerning the sharing and downloading of artillery targeting software, thereby deceptively passing malware as a legitimate software update. The SolarWinds' SUNBURST hack highlighted how even sophisticated software fortifications can fall prey to weak links in the software supply chain.

Ruses keep morphing over time. In the age of growing networked digital assets and cyberwarfare being farmed out to state-sponsored privateers, preventing cyberruses requires rethinking operational philosophy.

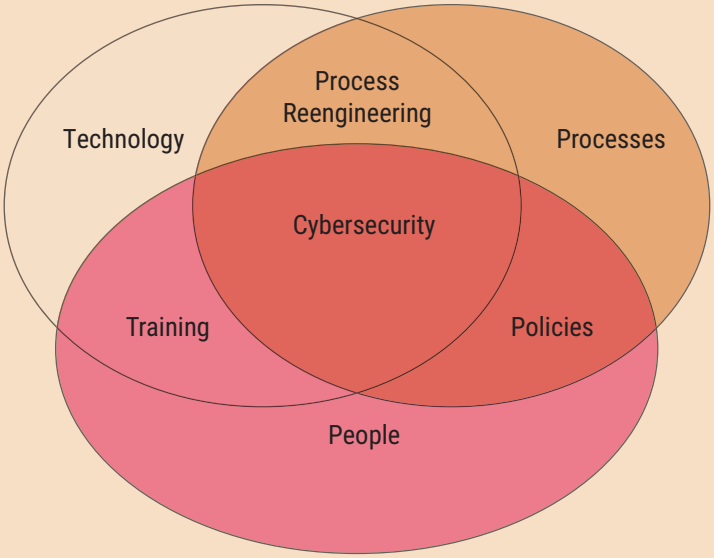
> "UNSURPRISINGLY, FAULTY PROCESSES AND FAULTY HABITS BECOME A WELLSPRING FOR CYBERRUSES."

Cybersecurity is not just a technological domain. Instead, cybersecurity is an evolving, global ecosystem comprising technologies, processes and people (**figure 1**).

Technology

Technology is the backbone of cybersecurity, and although it is necessary and central to cybersecurity, it often cannot be used as a sufficient solution on its own. Although cybersecurity technologies offer fortifications, they can be fooled by ruses.

Figure 1—Cybersecurity: A Confluence of Technology, People and Processes



Cybertechnologies are primarily designed for efficient automation based on discrete, conditional parameters for acting and reacting to triggers in a binary form. Yet even the best of such technologies can fall prey to a faulty process, especially when an attack source disguises itself as a legitimate actor or event.

Processes

Processes constitute the operational backbone of cybersecurity. An overreliance on technology without reengineering the underlying workflows and operational processes is analogous to greenwashing. Process reengineering and establishing process guidelines are integral to cyberoperations.

Process reengineering begins with mapping an entire process, whether an operational workflow or a software supply chain. Once a process is mapped, a cross-functional team examines each process activity for specific vulnerabilities and threats. For instance, some organization processes fail to deactivate access control privileges for interns who are being rotated across functions, creating a separation-of-duties compliance violation. A cross-functional team consisting of operational managers, human resources (HR), IT and finance (audit) meet together to reengineer the process to institute an intern-hand off procedure. The new intern-handoff procedure automatically deactivates specific resource views based on access privileges. In addition, all intern access is then based on a zero trust policy, with only multifactor authenticated trusted clients for access.

Process reengineering can help organizations further trust vendors by requiring enhanced verification across multiple nodes in the software supply chain. Deploying and rolling out cybersecurity technologies without reengineering the underlying process simply hides rather than eliminates the problem. Proactive process reengineering is the key to reducing lurking cyberthreats.

People

People, including employees, vendors and customers, constitute the human backbone of cybersecurity. Despite investments in technological fortifications and process reengineering, human error remains the weakest link in cybersecurity,[9] estimated to be the root cause of 95 percent of cybersecurity breaches.[10] People can be capricious and gullible, thus falling victim to cyberruses. Users often create simple passwords or write down and hide difficult passwords in easy-to-find places and can be spoofed easily to click unknown links out of curiosity, anxiety or greed.

Therefore, cyberwarfare ruses often begin with phishing and spoofing attacks intended to exploit and manipulate human psychology rather than technology. In December 2015, just after Russia annexed Crimea from Ukraine, Russia-sponsored

privateers allegedly sent a spoofed spear-phishing email to Ukrainian electricity IT staff. The email contained a malware Microsoft Word macro that led to a Ukrainian power grid blackout.[11] The 2014 Gautrain hack in South Africa relied on human errors of simple passwords and unlocked computers to steal passwords and install keylogger malware.[12]

Cybersecurity must acknowledge and address the importance of human behavior and biases while designing cybersecure systems. Although policies can guide human interactions and protocols in processes and workflows, more user-centric training can ensure that cybersecurity is understood and championed at the organization's grassroots.

Conclusion

The world and the economy are increasingly becoming more connected. The compounded effect of the COVID-19 pandemic has forced countries and organizations to pivot to digitally transform their operations. But breakneck digital transformation without a secure defense of digital assets is a recipe for cyberattacks.

Sophisticated, state-sponsored perpetrators have seized this opportunity to lay the groundwork for cyberwarfare.

As state-sponsored privateers create cunning cyberruses for disruption or ransom, organizations must think beyond cybersecurity technology investments. Securing the cybergates requires more focus on people (including vendors and consumers) and process errors that can rapidly become the weakest links in the cyberwarfare defense.

In an age marked by growing digital connectivity across critical economic and operational infrastructures, securing the borders requires more than just firewall fortifications.

Cyberwarfare underscores the need for revisiting organizational processes, culture and paradigms that are capitalized and leveraged by state-sponsored perpetrators. Instead of reactive technical fixes based on a "wait, watch, react" ideology, there is a need for a process reengineering of organizational operations and culture to build and maintain preventive readiness. Only then can one stay ahead of state-sponsored APTs from privateers and their ruses.

"BREAKNECK DIGITAL TRANSFORMATION WITHOUT A SECURE DEFENSE OF DIGITAL ASSETS IS A RECIPE FOR CYBERATTACKS."

Endnotes

1 Adams, S.; "Battle of Cadiz," Encyclopedia Britannica, *https://www.britannica.com/event/Battle-of-Cadiz-1587*
2 *Ibid.*
3 Datta, P.; "Hannibal at the Gates: Cyberwarfare and the SolarWinds SUNBURST Hack," *Journal of Information Technology Teaching Cases*, SAGE, 12 March 2021
4 American Battlefield Trust, "Yorktown: Siege of Yorktown," *https://www.battlefields.org/learn/revolutionary-war/battles/yorktown*
5 *Op cit* Adams
6 Volk, D.; "Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report," Reuters, 22 December 2016, *https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU*
7 *Op cit* Datta
8 Santayana, G.; *The Life of Reason*, Charles Scribener's Sons, USA, 1905
9 Datta, P.; E. Diffee; "Cybersecurity: The Three-Headed Janus," *Journal of Information Technology Teaching Cases*, 1 November 2018
10 *Security Magazine*, "95 Percent of Successful Security Attacks Are the Result of Human Error," 19 June 2014, *https://www.securitymagazine.com/articles/85601-of-successful-security-attacks-are-the-result-of-human-error*
11 Zetter, K.; "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*
12 *Op cit* Datta