INNOVATIVE AND DISRUPTIVE TECHNOLOGIES

State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks

Jan Kallberg and Bhavani Thuraisingham, The University of Texas at Dallas

A few nation states have started leveraging the Internet for geopolitical state gains. Using the development of the battle tank as an analogy, the authors explore the Internet's militarization. The technology used is old, but the ideas are revolutionary.

Public sentiment seems to be that Internet security has continually increased over the past 20 years, and recent advancements in client computer security have contributed to a population that largely trusts, and is at ease with, the Internet. People use online banking, run their businesses in the cloud, and rely on net-supported transactions. The limited abilities and resources of early attackers largely contained most threats. Attacks were primarily carried out through digital smash-and-grab thefts of credit card numbers and personal information, resulting in marginal financial damage.

The entrance of state actors as attackers reverses the trajectory of Internet security and extends the potential for damage. The threat no longer engulfs just individuals and businesses but also entire nations.

Novel Use of Existing Technology

Nation states are starting to exploit the Internet for policy, geopolitical, and state gains, but applying novel strategies to old technology for such gains is nothing new.¹ Consider the armored tank, which was first introduced to the battlefield in 1916. The tank was used for two decades as a movable pill box (bunker) and machine-gun nest; it could move from the trenches and follow the infantry in the World War I strategy of position warfare. It wasn't until the German assault on France in 1940 that the armored tank became an integral part of the military strategy, directly affecting the conflict's outcome.

The Germans saw the armored battle tank's potential in helping them reach their geopolitical goals. Before blitzkrieg—the German concept of

mobile armored warfare—wars were fought in a linear manner: the infantry was at the front of the fighting line, followed by a line of artillery bombarding the enemy from a distance, followed by a logistic echelon supporting the artillery and infantry. At the start of World War II, the French and many other armies still subscribed to this concept of three lines of military units, where only the first unit had contact with the enemy.

A shift in thinking occurred when Colonel Heinz Guderian, along with others in the late 1920s and throughout the 1930s, realized that armored tanks could do more than just slowly move alongside an infantry trying to take a hill or set of trenches.^{2,3} Guderian realized that tanks could be used in massive numbers to attack enemy territory. Instead of using the tank to move military hardware in a tactical manner, the Germans transformed it into a vehicle to form an innovative overarching strategy.

The revolutionary idea with blitzkrieg was to strike deep with massive tank formations, ignoring the enemy infantry to plough through the artillery and attack the bakery. Indirectly taking the initiative and forcing the enemy to counteract deflated the enemy's line of defense and made their units easy prey for the armored units. It took battle tanks almost 25 years to reach the point of effective military use, but the main obstacle was never the technology. Rather, it was the inability to reconceptualize the existing technology.

Development of the military helicopter followed a similar path. The helicopter was invented in the 1930s, and in the late 1940s and early 1950s, the military started to use it as a truck that could move through air space. The military had helicopters for 20 years before it started using them as a significant weapon. Once the intellectual ceiling was broken, militarized helicopters quickly evolved into today's attack helicopters.

The Internet has experienced developments similar to those of the armored tank and helicopter and the intellectual ceiling for Internet militarization has been incrementally breaking since 2010.

Militarizing the Internet

Militarizing the Internet didn't require new technology or networking capabilities; rather, it required rethinking how the Internet application layer could be used for political or military gains. Stuxnet—the set of code that affected the Iranian nuclear centrifuges—is the product of such a change in thinking. Designing Stuxnet to target and deliberately damage the Iranian nuclear centrifuges turned an existing technology into a new cyberweapon. Applying this type of weapon, nation states could potentially attack industrial control systems, such as municipal waterworks or other local infrastructure, damaging a society's ability to function.

The increased number of SCADA (supervisory control and data acquisition) systems attacks are a product of the shift in the cyberattack modus operandi, from marginally funded cybercriminals are replaced with well-funded state actors with a completely different objective and agenda.¹ A state actor seeking an advantage over another state might attack the core industrial backbone of a targeted country in the hopes of creating havoc in the transportation and communication infrastructure. For the traditional threat, cybercriminals, this would be a pointless operation, which is why we now must quickly change how we view, design, create, and maintain information security and protect our assets connected to cyberspace.¹

A militarized Internet and the potential for intelligence and economic espionage, which could destabilize adversarial states, radically changes the fundamentals for cyberspace security. State actors could exploit weaknesses in national infrastructures and information systems as well as exploit the public's heavy reliance on the Internet.

Although the goal for individuals and criminal networks is usually financial gain, a state might seek to optimize its influence and power or avoid being overpowered by others. It thus has a vested interest in being able to destabilize the systems of other nations and could employ a full-system attack strategy instead of the traditional cyberattack, which seeks limited goals with a quick turnaround. Nation states have more time, resources, and opportunities, making them a far more capable perpetrator for covert cyberoperations.

Certain areas, previously sheltered from cyberattacks—such as the space-borne US global information grid—could be a target for state actors.⁴ A criminal network or hackers didn't stand to gain financially from attacking the US global information grid, and even if they could sell the accessed information, it wouldn't be worth the risk, given the repercussions if caught.

INNOVATIVE AND DISRUPTIVE TECHNOLOGIES

Thus, the satellite infrastructure wasn't considered vulnerable. Attacking the global information grid represents no quick financial gain for a criminal network or hackers, and any marginal gain from selling the information would be drastically outweighed by the repercussions of the act, which have left the satellite infrastructure untouched by serious and capable cyberattacks.

However, in 2011, William J. Lynn III, former US deputy secretary of defense, reflected on the US national security space strategy:⁵

The willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate.

A kinetic antisatellite missile attack against the US would catapult the missile-launching nation on a confrontational course likely to lead to war or other uncertain drastic repercussions. However, a cyberattack carries much less risk, and it would be significantly harder to identify the perpetrator with sufficient satisfaction to warrant sanctions from the international community.

Attacking the superpowers' space-borne grids presents an opportunity to undermine information supremacy and war-fighting abilities, with direct geopolitical consequences.

The Digital Maginot Line

John Fraser, a British editor, wrote in *The Spectator* after a major British security breach:⁶

Suddenly, the western Internet "firewalls" are looking like a digital Maginot Line, so vulnerable that amateur hackers [could] steal hundreds of thousands of secrets for fun. So what might a cyberarmy be able to achieve?

This analogy relates back to the history of the tank, when the French built the Maginot Line on their border with Germany to ensure the Germans couldn't successfully attack France after World War I. Work started in 1930, and this construction project was one of the largest of its time. However, the Maginot Line was based on a major flaw—the French assumed the attacker would use a designated path and thus planned on fighting in fortified positions along that path. Using the new mindset of armored and mobile warfare, the Germans took another route, and the French endured one of history's most humiliating defeats.

The entrance of state actors into cyberoperations represents the same drastic change of mindset and concept as the Germans using mobile armored warfare to overrun French defenses in 1940. A digital Maginot Line would be pouring in money and resources into a defensive position that assumes that cyberattacks occur as expected. The vast effort in cybersecurity today is placed on addressing the threats of the past, where a few unfunded individuals pound a single point of system entry using often crude tools to find configuration errors.

Information assurance strategies thus resemble trench and position warfare, fought from fixed positions in a known terrain using hardened positions and pre-assessed planning. The hardened system defends against a few limited attacks trying to penetrate a specific sector, server, or area. We can't continue to focus on information assurance.⁶ By continuously hardening systems, a false sense of control and security is maintained, mainly based on the earlier attacker profile with single individuals or small criminal efforts penetrating the system. State actors have far more options to attack a system than solely trying to penetrate a firewall, so we need to redesign and restructure cybersecurity from a systems perspective.

he well-funded and geopolitically driven militarization of the Internet is a recent development—and represents a major shift in the related risks and threats. Security analyst Dan Geer has said that researching cybersecurity requires embracing the unknown⁷—in other words, cybersecurity researchers must step out of their comfort zone of traditional IT security, taking a higher-level systematic view of system security.

Political scientist Kenneth N. Waltz said that the power with nuclear arms isn't what you do with them but instead what you can do with them.⁸ Similarly, a state could use the mere threat of cyberoperations to deter other states from taking certain actions. However, once states engage their resources in cyberoperations, universities and intelligence agencies can become armories,⁹ and defense industries can receive contracts to identify weaknesses in foreign systems, redefining how we address cybersecurity.

References

- J. Kallberg and B. Thuraisingham, "From Cyber Terrorism to State Actors" Covert Cyber Operations," Strategic Intelligence Management—National Security Imperatives and Information and Communications Technologies, Butterworth-Heinemann, 2013, pp. 229–233.
- 2. H. Guderian, Achtung—Panzer! The Development of Armored Forces, Their Tactics, and Operational Potential, translation by C. Duffy, Arms and Armour, 1992.
- J.J. Mearsheimer, Liddell Hart and the Weight of History, Comstock Pub Assoc, 1988.
- J. Kallberg, "Designer Satellite Collisions from Covert Cyber War," *Strategic Studies Q.*, Spring 2012, pp. 129–146.
- W.J. Lynn III, "A Military Strategy for the New Space Environment," *Washington Q.*, vol. 34, no. 3. 2011, pp. 7–16.
- F. Nelson, "China's Spy Network," *The Spectator*, 4 Dec. 2010; www.spectator.co.uk/features/6507703/ chinas-spy-network.
- D. Geer, "A New Cybersecurity Research Agenda (In Three Minutes or Less)," *Threat Post*, 7 Nov. 2011;

https://threatpost.com/en_us/blogs/new-cybersecurity-research-agenda-three-minutes-or-less-110711.

- K.N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Rev.*, vol. 84, no. 3, 1990, pp. 731–745.
- J. Kallberg and B. Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Forces Q.*, vol. 68, no. 1, 2013, p. 53; www.ndu. edu/press/cyber-operations.html.

Jan Kallberg is a research scientist and lead at the Cyber Operations Research Lab at the Cyber Security Research and Education Institute (CSI) in the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas. His research interests include offensive cyberoperations and societal stability. Kallberg received his PhD in public affairs from the University of Texas at Dallas. Contact him at jkallberg@utdallas.edu.

Bhavani Thuraisingham is a Louis A. Beecherl, Jr. Distinguished Professor and an executive director of the Cyber Security Research and Education Institute (CSI) in the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas. Her research interests include information assurance, system theory, and secure dependable data management. Thuraisingham received her PhD in theoretical computer science from University of Wales and the higher doctorate of engineering from University of Bristol. Contact her at bhavani. thuraisingham@utdallas.edu.

ADVERTISER INFORMATION • MAY/JUNE 2013

Advertising Personnel

Marian Anderson: Sr. Advertising Coordinator; Email: manderson@computer.org Phone: +1 714 816 2139 | Fax: +1 714 821 4010 Sandy Brown: Sr. Business Development Mgr. Email sbrown@computer.org Phone: +1 714 816 2144 | Fax: +1 714 821 4010

Advertising Sales Representatives (display)

Central, Northwest, Far East: Eric Kincaid Email: e.kincaid@computer.org Phone: +1 214 673 3742; Fax: +1 888 886 8599

Northeast, Midwest, Europe, Middle East: Ann & David Schissler Email: a.schissler@computer.org, d.schissler@computer.org Phone: +1 508 394 4026; Fax: +1 508 394 1707 Southwest, California: Mike Hughes Email: mikehughes@computer.org Phone: +1 805 529 6790

Southeast: Heather Buonadies Email: h.buonadies@computer.org Phone: +1 973 585 7070; Fax: +1 973 585 7071

Advertising Sales Representatives (Classified Line)

Heather Buonadies Email: h.buonadies@computer.org Phone: +1 973 585 7070; Fax: +1 973 585 7071

Advertising Sales Representatives (Jobs Board)

Heather Buonadies Email: h.buonadies@computer.org Phone: +1 973 585 7070; Fax: +1 973 585 7071