

Geopolitics: An Overlooked Influencer in Cyber Operations

[MalBot](#) 1 February 28, 2019, 9:15pm

***Editor's Note:** The following blog post is a summary of a presentation from RFUN 2018 featuring Jeannette Dickens-Hale and Danika Blessman of NTT Security.*

Key Takeaways

- Geopolitics helps us understand, explain, and predict international behavior.
- From a cyber perspective, understanding geopolitical influences can help organizations predict and prepare for serious cyber threats.
- Analysis of cyber activity over the past decade demonstrates a clear link between geopolitical motivations and state-sponsored cyber campaigns.
- Geopolitical intelligence should be combined with traditional threat intelligence-gathering techniques to help organizations determine how, when, and where they are likely to be targeted.

The [vast majority of cyberattacks](#) are financially motivated, but not all cyberattacks are about money. While attacks by state-sponsored threat groups are certainly in the minority, they also can be far more dangerous than those perpetrated by petty criminals.

Back in October 2018, we held our seventh annual [Recorded Future User Network](#) (RFUN) conference in Washington, D.C. During the conference, attendees were treated to a presentation on geopolitics and its influence on cyber operations by Jeannette Dickens-Hale and Danika Blessman, two senior threat intelligence analysts from NTT Security.

The pair have an extensive history in traditional intelligence analysis, including for NORAD and the U.S. military. During the presentation, Dickens-Hale and Blessman explained how geopolitics fits into the cyber domain, and how an understanding of geopolitical motivations can help organizations predict and prepare for serious cyber threats.

What Is Geopolitics?

The presentation kicked off with a simple definition of geopolitics:

1. The study or the application of the influence of political and economic geography on the politics, national power, foreign policy, etc., of a state.
2. The combination of geographic and political factors influencing or delineating a country or region.
3. A national policy based on the interrelation of politics and geography.

Or, as Blessman put it during the presentation: “Geopolitics is a discipline designed to explain the intersection between people and place, and the impact they have on each other. It helps us understand, explain, and predict international political behavior — taking something unpredictable and making it a little more predictable.”

From a cyber perspective, understanding [geopolitical influences](#) can help organizations predict and prepare for serious cyber threats before they happen.

The Science of Geopolitical Motivation

Cyber activity is an appealing way for nation-states to achieve their objectives for one key reason: because it's so difficult to empirically attribute an attack to a specific nation, it's very unlikely that targeted nations will respond with real-world ("kinetic") military action.

To understand how geopolitical motivation influences cyber activity, it's helpful to see it in action. During the presentation, Blessman took the audience through a series of real-world examples from the past few years.

Syria

In April 2018, the U.S. [threatened military action](#) in Syria following a suspected chemical weapon attack on civilians near Damascus. In the immediate wake of this announcement, intelligence analysts observed a threat group known as the Syrian Electronic Army targeting Western media outlets.

The group has also previously [targeted media outlets in the U.K.](#) following their coverage of Syrian airstrikes in Raqqa.

North Korea

Historically, North Korea's cyber program has primarily been observed conducting traditional cyberespionage and utilizing disruptive or destructive techniques against geopolitical adversaries.

More recently, however, North Korean threat groups have been observed attacking SWIFT banking networks and bitcoin mining exchanges. While these attacks can likely be chalked up as a response to sanctions from Western nations, they serve the dual purpose of making money for the regime.

Iran

Originally, most Iranian cyber activity — mostly in the form of vandalism — was conducted by patriotic hacking groups. However, since [Stuxnet](#) (a worm developed by U.S. and Israeli agencies to disrupt the Iranian nuclear program), Iranian threat groups have focused primarily on retaliation.

For example, following the release of the inflammatory "Innocence of Muslims" video by an American pastor, Iranian hackers conducted denial-of-service (DoS) attacks against [a variety of U.S. financial institutions](#), including the New York Stock Exchange.

Over time, Iranian cyber capabilities have evolved considerably, leading to [revelations in 2014](#) that Iranian hackers had compromised government agencies and critical infrastructure in more than 16 countries.

China

Of all the nations involved in the cyber domain, China is among [the most active and advanced](#).

The Chinese government routinely produces a strategic document (known as its five-year plan) outlining the industries and projects that will be a national focus over the following five years. The current plan runs from 2016 to 2020, and focuses on (among other things) critical infrastructure, healthcare, and green energy.

As Blessman explained during the presentation: “Historically, China’s five-year plans have been a good indicator of which industries should keep their cyber defenses up, as their cyber activity generally aligns with the priorities in their five-year plan.”

Similarly, initiatives such as China 2025 — China’s stated intention to (among other things) reduce the country’s dependence on foreign technologies — can provide valuable insight into their likely cyber activities.

Since China is actively trying to develop its own cutting-edge manufacturing technologies, it should be no surprise that Chinese threat groups have often been observed targeting high-tech manufacturing organizations in the U.S.

Case Study: Russia’s State-Sponsored Cyber Operations

During the second half of the presentation, Dickens-Hale took the audience through a more detailed geopolitical case study.

In recent years, [Russia has been extremely busy in the cyber domain](#), and Dickens-Hale covered the activities of two highly active groups from Russia’s largest foreign intelligence agency: GRU units 26165 and 74455 (the threat actor group APT28, also known as Fancy Bear, was recently identified as these two GRU units by the United States Special Counsel in a 2018 indictment). First, she noted the groups’ cooperative focuses:

- **Unit 26165:** Cyber operations and data extraction
- **Unit 74455:** Disseminating information in a way that benefits Russia

The following are some of the Russian cyber campaigns described by Dickens-Hale during the presentation.

Influencing the 2016 Presidential Election

The first truly high-profile example of the work conducted by GRU Units 26165 and 74455 was their attempt to influence the result of the U.S. presidential election in 2016.

Operatives from Unit 26165 used highly advanced social engineering campaigns and exploited vulnerabilities to gain access to target networks, and used malware such as X-Agent and X-Tunnel to steal huge quantities of sensitive data. Later, they used a tool called CCleaner in an attempt to erase any evidence of their presence.

During the course of this campaign, Unit 26165 used a global network of computers to conduct their attacks and hacked a wide variety of organizations related to the election. State election boards and local election boards were heavily targeted, along with a software company involved with voter registration.

Once they had the data they needed, Unit 74455 used [DC Leaks and Guccifer 2.0](#) to disseminate information in a manner designed to influence U.S. voters.

Retaliation Against Olympic Ban

The ban on Russian athletes competing in the Olympics following accusations of doping directly influenced GRU cyber campaigns against a variety of international sports organizations.

Targets of GRU cyberattacks included:

- The U.S. Anti-Doping Agency (USADA) — Colorado Springs, Colorado
- The World Anti-Doping Agency (WADA) — Montreal, Canada
- Canadian Centre for Ethics in Sports, (CCES) — Ottawa, Canada
- International Association of Athletics Federations (IAAF) — Monaco
- The Court of Arbitration for Sport (TAS/CAS) — Lausanne, Switzerland
- The Fédération Internationale de Football Association (FIFA) — Zurich, Switzerland

Retaliation Following Poisoning of a Russian Double Agent in the UK

In March of last year, a former Russian spy and his daughter were poisoned in Salisbury, U.K. by Russian operatives using the nerve agent Novichok.

In response to their role in identifying the nerve agent, GRU conducted a series of cyberattacks against organizations in the Netherlands and Switzerland:

- Organization for Prohibition of Chemical Weapons (OPCW)
- Spiez Swiss Chemical Company

The Spiez Swiss Chemical Company is accredited with the OPCW and was responsible for analyzing the chemicals used to conduct the poisoning.

Using Geopolitical Intelligence

At this point, an important question arises: As interesting as these case studies are, can understanding geopolitical influences and motivations really help organizations predict and protect against cyberattacks? Dickens-Hale and Blessman believe it can.

“If you understand the motivations of state-sponsored threat groups, you can figure out if you’re likely to be attacked. For example, if you’re operating in an industry that is of interest to Russia or China, you have to be aware that you could be a target,” Dickens-Hale explained.

The key is to combine an understanding of geopolitical influences with traditional intelligence-gathering techniques. The “who” and “why” are important factors, but in order to predict and protect against cyberattacks, you also need to determine how and when they are likely to be carried out.

If you’ve determined that your organization may be a [target for a given agency or group](#), you can use that hunch to inform more focused intelligence gathering — for example, by monitoring social media chatter or

dark web activity.

Combine this with the outputs of traditional intelligence analytics and research, along with an understanding of your organization's network architecture, and you're in a strong position to identify sensible security enhancements.

Stay Ahead of Targeted Threats

One of the ways you can find out about active threat actors — including their preferred target industries and TTPs — is by subscribing to our free [Cyber Daily](#).

When you sign up, you'll receive daily emails with the latest threat indicators as reported by Recorded Future, including:

- Top targeted industries
- Top threat actors
- Top exploited vulnerabilities
- Top malware
- Top suspicious IP addresses
- Top cybersecurity news

[Subscribe today](#) and start using this useful intelligence to stay ahead of cyber threats.

The post [Geopolitics: An Overlooked Influencer in Cyber Operations](#) appeared first on [Recorded Future](#).

Article Link: <https://www.recordedfuture.com/geopolitical-cyber-operations/>