Drexel Hamilton
A Service-Disabled Veteran Owned & Operated Business

Outside the Wire
Ransomware, Geopolitics, and Lessons from History

Photo Credit: Datto

History is always a strong guide to inform our current geopolitical sagas. Recent history is even better. The Global War on Terror dominated foreign policy for most of the 21st Century. But it has been overshadowed by the "war" on cyber threats. Unfortunately, both "wars" are mischaracterized.

The Prussian military historian Carl von Clausewitz described war as an extension of politics by violent means. Clausewitz's definition of war remains one of the central theories that dominates martial studies. The proper definition is more important than one might imagine. In fact, it is the crucial distinction that can prevent a needless war. But most pundits and media "analysts" do not know this definition and probably have never heard of Clausewitz. This is where we find the current state of historical illiteracy to be frightful.

A Snapshot of Recent History

One of the premises behind the Iraq war was that Saddam Hussein was harboring terrorists most notably the eventual founder of ISIS, Abu Musab al-Zarqawi. When the U.S. made a case to the U.N. Security Council for invading Iraq, Secretary of State Colin Powell famously used a "connection" between Zarqawi and Saddam Hussein as justification for intervention. However, there was no connection between the two. In fact, Zarqawi had moved to northern Iraq after attempting to join the Taliban in Afghanistan. Saddam's intelligence was monitoring Zarqawi, but they were not associated with him in any meaningful way. At the time the CIA had an opportunity to take out Zarqawi but were denied based on the imminent invasion. Over the course of the following years, Zarqawi and his ruthless organization, known at the time as Al-Qaeda in Iraq (AQI), would reign terror in Iraq. The once nascent terrorist group would grow into a global terrorist organization that eventually captured large amounts of territory in Iraq and Syria.

What is the Point of this Cautionary Tale?

The point is that it is important to understand where regimes are connected to non-state actors and the relationships between them. With respect to Russia and the recent spate of ransomware "attacks", it is critical to understand that the regime itself likely has no or little connection to criminal enterprises engaged in ransomware. Furthermore, what incentive would the Russian military have to use cheap and easily obtainable cyber tools (i.e. the ones used for ransomware) to target a U.S. company that had poor security protocols for a mere $5 million dollars? There is no logic to that type of geopolitical risk.

Additionally, it is important to make the distinction that the industrial control systems were not hacked. Colonial Pipeline's computer networks were hacked which led the company to decide to shut down their operations out of caution. In recent years when industrial control systems have been hacked for geopolitical purposes, the hacks are incredibly sophisticated with cyber tools that took years of development. For example, the U.S. use of Stuxnet against the Iranian nuclear centrifuges is a case of a carefully developed cyber weapon that was used for a very specific geopolitical goal i.e. the disruption of Iran's nuclear capabilities.

The Colonial Pipeline Smyrna Station.
Photo Credit: Associated Press

In the lead up to the summit between President Biden and Vladimir Putin, a lot was made of Biden confronting Putin over "cyberattacks." While the cybercriminal groups might be based in Russia, this is different from Russia pursuing ransomware as means to a geopolitical end. And what would Russia's geopolitical end-state have been to take $5 million of Colonial Pipeline's money? Mass confusion in the United States? Would Putin think that this would make the U.S. less inclined to push for Ukraine's inclusion in NATO? The costs do not seem to add up to the benefits.

On the other hand, the SolarWinds hack might be associated with the Russian government. What would their end-state be in that case? Espionage. The same thing that every country engages in. This is simply James Bond meets the Internet. SolarWinds was not an "attack" though. The U.S. and Russia are both engaged in cyber espionage, and it is doubtful that there will be a meaningful truce on this front.

The big takeaway is to remember that there are multiple layers of nuance in geopolitics. Things cannot be painted with a broad brush or more catastrophe is likely to follow. In the meantime, every organization connected to the Internet is best advised to make sure their employees are using two factor authentication, not clicking on suspicious e-mails, using strong passwords, and having network engineers segregate networks to prevent ransomware from spreading.