Tony Janus

NET-100 Computer Ethics

10/06/2024

The Iranian Cyber Army

This week's focus is on the topic of cyber attacks against US infrastructure, specifically the Iranian "cyber army" and their growing capabilities. This is a dryer, more fact-focused subject, with its framing given a lesser emphasis on morality and ethics. As a result, the following conversation will come across as more descriptive and less philosophical in tone, though that does not invalidate its importance.

The Iranian cyber army appears to be composed of various groups with ties to the Iranian government, including those of freelancers, criminal organizations, and those under state employ. A number of these groups have been identified and named publicly. Some of these include the Izz ad-Din al-Qassam Cyber Fights, a group who claimed responsibility for the attacks against U.S. financial institutions in 2012 using DDoS attacks (Directed Denial of Service, or a method of overwhelming web servers with traffic to prevent their usage by their intended audience), the groups APT33 (aka Elfin, Refined Kitten, Holmium), APT35 (aka Phosphorus, Charming Kitten, Ajax Security), and APT39 (aka Remix Kitten, Remexi, Cadelspy, Chafer, Cobalt Hickman, and ITG07), (APT being an acronym which stands for Advanced Persistent Threats), all three groups being linked with the Iranian government, and the Iranian Dark Coders Team which is a hacker collective of freelancers and criminal elements that has not been tied to the Iranian

government, proving that Iran relies not only on its own operatives, but also freelancers who are in ideological alignment with them.

These groups are only a handful of those operating within the country, yet they've claimed responsibility for a number of high-profile hack events over the past decade and a half, both against civilians as well as government targets. The APT33 group was linked to the Iranian government by FireEye, a cybersecurity firm I spoke about in this week's discussion post, and have been found to conduct "espionage operations against aviation, military, and energy targets in the United States, Saudi Arabia, and South Korea." The APT39 group, active since 2014, has focused more on economic targets, stealing "personnel and private business information from telecommunications companies and airlines." The Iranian Dark Coders Team held a greater emphasis on propagandization, attacking websites and seeding them with pro-Hezbollah and pro-Iran propaganda in 2012.

The attacks launched by Iran and their cyber army have been numerous over the years and pose a major concern not only to American safety, but to our economy and our way of life. While I acknowledge there have been attacks against military and government targets, which are of course very serious, I'm more concerned about the threat to intellectual property.

War is still often times painted with language that gives the impression of nations fighting over land disputes. While news sources rarely make such claims, I cannot help but have those associations due to my exposure to historical education and media presentation, both fictional and non-fiction. Wars of previous centuries were fought for access to resources, supply routes, and proximity defenses. We learned in school about the Germans eating up parts of

Europe to expand its territory, and likewise with the Ottomans, the Mongols, etc… all throughout history. Even in recent years, Russia has invaded Ukraine to take back land they believe is theirs and reincorporate the people living there into the Russian population. Works of fiction like The Lord of the Rings contain grand battles over territories and the proverbial villain who wants to "take over the world."

These representations of war leave a mark on the public's perception of what war is, so even if we consciously know otherwise, we still have a habit of speaking like nations are in conflict over some tangible resource. In reality, modern war is ideological and economic, with each "side" viewing the other as manifestations of moral, cultural, and/or theistic evil. Hacker groups, both state-endorsed and freelance, attack economic targets and infrastructure, which harm the nation's GDP, their supply chain, and the businesses operating within the nation's bottom line. Many attacks are focused on stealing technologies and intellectual properties, giving the sponsoring nation a technological and economic advantage it otherwise would not have. This leads to hostile nations who are behind in their societal and technological progress to catch up with more advanced nations, gaining access to advantages they may not use responsibly as they never experienced the mistakes and lessons learned through those technologies' development.

These threats are not just the concern of government entities, but of the public as well. If we lose our industrial and economic advantages, like when China steals patented technology and replicates it at a lower cost, this ultimately hurts the average American. Companies lost profits when this happens, which leads to less cash flow through the nation. With less capital fueling the economic machine, there is less innovation and fewer developments, exports fall as

economic allies gravitate towards less expensive options, and this affects the pocketbook of the average citizen.

The attacks against the U.S. and its interests by the Iranian cyber army is less frequently talked about than those from Russia, China, or North Korea, but are equally important and just as harmful, if not more so simply due to the fact they are given less attention. State agencies may be on alert, but the public does not hold the same perspective or sense of urgency regarding Iran, with Russia and China taking center stage in public discourse. This allows Iran the opportunity to take advantage of our blind spots, which they have been doing for years, and are likely to continue to do if we don't re-assess and re-adjust.

Sources:

- The Invisible U.S.-Iran Cyber War – Andrew Hanna, United States Institute of Peace (https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war)
- The World's Best Hackers: Why Iran Is A Bigger Threat To The U.S. Than Russia, China or North Korea – Cristina Maza, Newsweek (https://www.newsweek.com/best-hackers-world-iranian-cyber-spies-indicted-trump-859023)