SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog December 2020

Topics covered in this issue:

- SolarWinds Hack - an unprecedented digital intrusion into a significant number of private and public entities, primarily in the United States Privacy concerns of Covid vaccination patient data.

The SolarWinds Hack

The resource list for December 2020 focuses exclusively on what has become known as the SolarWinds hack, an unprecedented digital intrusion into a significant number of private and public entities, primarily in the United States, that will prove to have significant ramifications as it pertains to the entire spectrum of cybersecurity considerations-including, but not limited to, legislation, retaliation, private-public sector interaction, national cyber defense capabilities and limitations, and the organizational/personnel structure of the current federal defense national security apparatus. These matters are of the utmost importance in the wake of such a significant digital intrusion as a new presidential administration under President Joe Biden is set to assume control of the federal government in mid-January of 2021, wielding the ability to reshape the nation's cybersecurity posture and hierarchy.

This report will be presented in an altered format from previous resource lists prepared by this author for Ward Sciences and Consulting LLC, as a means to synthesize the examined sources into a coherent and sequential narrative. The sources will be presented in list form beneath this paragraph, and cited parenthetically throughout the report. The resources cited in this report are as follows:

-Newman, L. (2020, December 19). How to Understand the Russia Hack Fallout. Retrieved December 28, 2020, from https://www.wired.com/story/russia-solarwinds-hack-targets-fallout/

-Sanger, D., Perlroth, N., & Barnes, J. (2021, January 02). As Understanding of Russian Hacking Grows, So Does Alarm. Retrieved January 4, 2021, from https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

John Ward – Cyberblog December 2020

-Sanger, D., & Perlroth, N. (2020, December 19). Trump Contradicts Pompeo Over Russia's Role in Hack. Retrieved December 24, 2020, from https://www.nytimes.com/2020/12/19/us/trump-contradicts-pompeo-over-russias-role-in-hack.html

-Smith, B. (2020, December 18). A moment of reckoning: The need for a strong and global cybersecurity response. Retrieved January 17, 2021, from https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

-Sanger, D. E. (2019). The perfect weapon: War, sabotage, and fear in the cyber age. New York: Broadway Books.

-Greenberg, A. (2020). Sandworm. Random House US.

-Bing, C., & Menn, J. (2020, December 08). U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools. Retrieved December 20, 2020, from https://www.reuters.com/article/fireeye-cyber/us-cybersecurity-firm-fireeye-discloses-breach-theft-of-hacking-tools-idUKKBN28I34H?edition-redirect=uk

-Nakashima, E & Timberg, C (2020, December 15). The US government spent billions on a system for detecting hacks. The Russians outsmarted it. Retrieved December 20th, 2020, from https://www.washingtonpost.com/national-security/ruusian-hackers-outsmarted-us-defenses/2020/12/15/3deed840-3f11-11eb-9453-fc36ba051781_story.html

On December 8th, 2020, Reuters published an article reporting that FireEye, “one of the largest cybersecurity companies in the United States” (Bing & Menn, 2020) had been hacked and that the hackers had made off with some of their proprietary hacking tools (Bing & Menn, 2020). These tools were later revealed to be FireEye’s “red team” tools, which FireEye uses to digitally “probe” their clients in an effort to find cybersecurity vulnerabilities, of which they are then notified (Sanger and Perlroth, 2020). The initial Reuters article indicated that FireEye suspected that the theft had the hallmarks of a “government-backed hacking operation” (Bing & Menn, 2020), a sentiment echoed by Matt Gorham, the assistant FBI director of the Cyber Division. (Bing & Menn, 2020). The article cites an unnamed former Department of Defense official who specified that they believed that the most likely perpetrator was Russia (Bing & Menn, 2020).

John Ward – Cyberblog December 2020

In the weeks following the initial Reuters report, a more complete understanding of the nature of the intrusion began to take shape, as well as a more complete understanding of the scope of the intrusion. The nature of the intrusion is that malicious software was implanted into targeted platforms via a tainted patch for network management software developed by the IT management company SolarWinds (Newman, Lily H., 2020). Once the software was implanted (the software is not malicious in-and-of-itself), the hackers had the capability to activate it remotely and upload further malware, gaining access to the platforms (Newman, Lily H., 2020). In some cases, it appears that this malicious "backdoor" was installed, but never exploited, laying dormant (Newman, Lily H., 2020). In many other cases however, it appears that these backdoors were eventually activated and used for reconnaissance/theft purposes (Newman, Lily H., 2020).

As mentioned above, the primary means of delivery for this malicious intrusion was a patch released by the company SolarWinds for their Orion network management software, a patch that was available for download between March and June of 2019 (Newman, Lily H., 2020). According to SolarWinds in an SEC breach filing, they have 300,000 customers (Newman, Lily H., 2020). Of those customers, it is believed that only those who utilized their Orion software, and of those customers, only those who downloaded the specific version of the tainted patch, were affected (Newman, Lily H., 2020). SolarWinds, in the same SEC breach filing, indicated that they had notified their approximately 33,000 Orion customers of the threat, of whom they believed that approximately 18,000 of the were vulnerable (Newman, Lily H., 2020). It is believed that the original breach may have occurred as early October of 2019, meaning that it went undetected for approximately 14 months (Newman, Lily H., 2020).

SolarWinds as a company is not well-known, but their software is near-ubiquitous throughout the public and private sectors. As mentioned earlier, they estimate that they have approximately 300,000 entities as customers. These customers include a myriad of federal agencies, of which it is believed over 250 have been affected (Sanger, Perlroth & Barnes, 2021). This includes the Departments of Commerce, Treasury, Homeland Security and Energy (Newman, Lily H., 2020). It is impossible to overstate how significant this access could be for a malicious actor-as just one example, the Department of Energy is responsible for the United States' nuclear arsenal. A tremendous amount of private entities are affected as well, with Microsoft president Brad Smith indicating that as of December 17th, it had notified 40 customers of a deep intrusion-including customers in Canada, Mexico, Belgium, Spain, the UK, Israel, and the UAE.

Curiously enough, they did not find any evidence of affected networks within Russia. (Smith, 2020). These customers were identified by analyzing Microsoft Defender software on computers belonging to clients who also downloaded the Orion patch (Smith, 2020). Even more troubling, subsequent examinations of the intrusions have found that the SolarWinds patch more than likely not the only means of intrusion for these hackers-CISA released an alert on 12/17/2020 that indicated "initial access vendors other than the SolarWinds Orion platform" were vectors of access for the malicious actors, and the cybersecurity company CrowdStrike stated that they had been affected by the same intrusion through a company that resells Microsoft software (Sanger, Perlroth & Barnes, 2021).

The response to these intrusions has largely come from the private sector. FireEye, in partnering with other firms including Microsoft, has begun to publish "indicators of compromise", such as IP addresses and DNS record responses associated with the intrusions (Newman, Lily H., 2020). Concerned entities can then check their network activity to verify if it is exhibiting any of the signs of this particular intrusion. They are also working to develop a "kill switch" for the malware, done to seize control of the IP addresses that the malware communicates with so that it is unable to receive commands (Newman, Lily H., 2020). However, there is some concern that as the technical details are publicized, hackers who were unoriginally affiliated with the intrusion could piggyback on the backdoors (Newman, Lily H., 2020).

The scope, nature, and success of this cyberattack raises almost countless issues about the nation's cybersecurity posture, and highlights significant concerns with almost every aspect of effective cybersecurity policy and practice, both in the public and private sector. The first aspect of this intrusion that must be examined is the primary vector of access, SolarWinds. SolarWinds, a Texas-based company, has justifiably been under significant scrutiny since the intrusions were made public. The New York Times interviewed several current and former employees of the company, and the responses were troubling and indicate an environment in which cybersecurity was not prioritized-an oversight that has proven to be catastrophic.

John Ward – Cyberblog December 2020

According to the NYT report, SolarWinds' chief executive is a man named Kevin B. Thompson, who was an accountant by training and had previously been a CFO (Sanger, Perlroth & Barnes, 2021). The report indicates that Mr. Thompson, with a mindset based primarily on finances, forewent a number of common-practice security measures in an effort to cut costs, only beginning to add important security measures in 2017 when they were compelled to by the enaction of a European privacy law (Sanger, Perlroth & Barnes, 2021)-these measures included the hiring of a chief information officer and a vice president of security architecture (Sanger, Perlroth & Barnes, 2021). The report included statements from a former SolarWinds cybersecurity consultant, Ian Thornton-Trump, who said that in 2017 he communicated to SolarWinds management that they were still susceptible to "a cybersecurity episode that would be catastrophic", and resigned when he observed that his recommendations were ignored (Sanger, Perlroth & Barnes, 2021). Furthermore, the report indicated that SolarWinds continued to offer the tainted patch for several days after the attack was publicized (Sanger, Perlroth & Barnes, 2021).

As unconscionable as these cybersecurity lapses from SolarWinds seem, they are not the only victimized entity to examine in the aftermath of these intrusions. Although not nearly as culpable as SolarWinds, the developer, vendor and provider of the primary vector of access, the immediate aftermath of the attack indicated that many of their customers were not as cybersecurity focused as may be expected in the current environment. It would be incorrect to point any of the blame at these customers, for a variety of reasons-even FireEye, one of the premier cybersecurity companies in the world, only realized that there was an issue when the hackers performed a brazen act-the theft of their "red team" hacker tools. The nature of the intrusions was extremely sophisticated, and clearly very difficult to detect. Furthermore, the nature of the delivery of these backdoors was that it affected those who were practicing good cyber hygiene-the downloading and implementation of up-to-date patches is a cornerstone of good cybersecurity policy, and these backdoors were delivered via a legitimate patch. However, the fact that SolarWinds software was so ubiquitous, particularly within the federal government, without any scrutiny of the developer (whose lax cybersecurity posture should have raised significant red flags prior to utilizing the software), indicates a significant lack of due diligence, as well as an over-reliance on one particular platform throughout several federal entities, so that when something of this nature occurs, the effect is not isolated to one or two entities but almost the entire federal government. Of particular note, the New York Times report cited in the above paragraph states that most of the SolarWinds customers contacted by the NYT were not aware that they were even using SolarWinds software (Sanger, Perlroth & Barnes, 2021).

John Ward – Cyberblog December 2020

We have examined how lax cybersecurity practices from the developer, and lack of due diligence from the customers, contributed to the current situation. This portion of the paper will examine this matter from the viewpoint of this intrusion as being a national security issue-how was it not prevented or detected for so long, and what are the ramifications for the national security cybersecurity community moving forward? Who is responsible, and how will they be dealt with? These are important questions as a new administration ascends to the seat of power, and bears the responsibility from an ever-evolving threat in the cyber arena.

What are the United States' current defense capabilities, and why were they unable to prevent or detect this monumental intrusion? This is a multifaceted examination, with both theoretical and tangible aspects, and will consider both the technological capabilities of the United States, as well as the doctrinal decisions made regarding cybersecurity.

In a Washington Post article written a week after the hack became public, Ellen Nakashima and Craig Timberg reported on Einstein, the primary apparatus used by the United States government to detect malware attacks and intrusions. Einstein is operated by CISA under the auspices of the Department of Homeland Security. Although Einstein has cost billions of dollars to this point, it has major blindspots that were exploited by the perpetrators of what has become known as the SolarWinds hack (Nakashima & Timberg, 2020). Einstein's primary function is "finding new uses of known malware and also detecting connections to parts of the internet used in previous hacks" (Nakashima & Timberg, 2020). This means that Einstein is not designed to identify new malware or vectors of attack, and instead relies on previously identified cyberattack tools and operations to identify when they are attempted to be used again (Nakashima & Timberg, 2020). While Einstein is able to identify variations and augmented versions of these previously-used components, it is unable to detect entirely new malware or vectors of attack (Nakashima & Timberg, 2020). It is unusual for a cyberattack or intrusion to be comprised entirely of unprecedented and previously-unknown components-such an attack would require a significant amount of sophisticated technological capability and the vast resources needed to develop them-but as SolarWinds has proven, it is not impossible. In the aftermath of the SolarWinds intrusion, CISA told congress that Einstein did not have the capabilities to flag the SolarWinds attack (Nakashima & Timberg, 2020). A 2018 Government Accountability Office report had previously highlighted this particular shortcoming (Nakashima & Timberg, 2020). The report prognosticated that by 2022 Einstein would have the capability to "identify any anomalies that may indicate a cybersecurity compromise", and clearly that capability was not developed and implemented by late 2020 (Nakashima & Timberg, 2020).

John Ward – Cyberblog December 2020

Doctrinal policy and operational decisions also need to be examined in the wake of the SolarWinds hack. General Paul M. Nakasone is the current Commander of the United States Cyber Command (he is also the director of the NSA and the Chief of the Central Security Service). General Nakasone's primary cybersecurity tactic is what is described as "defending forward"-in which offensive and pre-emptive cyberactions are taken to hack into adversaries networks to detect any potential operations against the United States (Sanger, Perlroth & Barnes, 2021). In the case of the SolarWinds intrusion, this tactic clearly did not detect the threat. It is important to note that while there are many critics of General Nakasone's strategy of being "too much offense, too little defense", Homeland Security and the DHS are prohibited from entering or defending private sector networks (Sanger, Perlroth & Barnes, 2021), a fact that was exploited by the perpetrators of the SolarWinds attack.

The New York Times suggests that there may have been other factors in the success of the SolarWinds attack. The 2016 elections were marred by the belief that Russia had digitally influenced them. The national security community, as well as private companies such as Microsoft and FireEye, prioritized a robust cyber defense for the 2020 elections, and was largely successful. However, the New York Times suggests that the amount of resources and attention given to the cyber defense of the 2020 elections allowed the perpetrators to focus their attention on other entities of the United States, such as those targeted by the SolarWinds hack (Sanger, Perlroth & Barnes, 2021). Furthermore, the New York Times reported that one of Mr. Thompson's cost-cutting measures at SolarWinds was to outsource engineering to the Czech Republic, Poland, and Belarus, where their product may have been more susceptible to foreign (primarily Russian) interference (Sanger, Perlroth & Barnes, 2021). While neither of these factors have been verified, they are important to consider moving forward.

An essential component of an examination of the SolarWinds hack is to identify the culprit or culprits. It is largely believed that the SolarWinds attack was a state-sanctioned Russian attack, probably perpetrated by the governmental intelligence organization known as the SVR (Newman, Lily H., 2020), although there have been dissenting opinions. It is essential that the culprit is publicly identified. A state-sponsored hacker, especially if it is a governmental agency, is unlikely to ever face justice in the United States, but a clearly identified perpetrator is a necessary step in allowing the American people to more clearly understand the threat the country is facing.

John Ward – Cyberblog December 2020

In his book Sandworm, author Andy Greenberg describes SVR in the following way while investigating their culpability in the DNC hack of 2016 "…engage(s) in extensive political and economic espionage for the benefit of the government of the Russian Federation…" (Greenberg, 2020 p. 116). The SVR, which is Russia's foreign intelligence service, is not the only Russian governmental organization that conducts these types of operations. The GRU, Russia's main intelligence organization, is perhaps more well-known to the general public, and was also implicated in the DNC hacks (Greenberg, 2020). According to the New York Times, the Dutch have been instrumental in helping the international community understand the SVR, having alerted the US to a previous intrusion, and having had broken in and accessed SVR systems for at least a year before being detected (Sanger, Perlroth & Barnes, 2021). This led to an assessment of the SVR as being "…not known for being destructive, (but) notoriously difficult to evict from computer systems it has infiltrated" (Sanger, Perlroth & Barnes, 2021).

The particular Russian governmental organization that is responsible for the SolarWinds hack is not as important to the general public as a firm understanding and official acknowledgement that it was Russia, and not a mysterious third party or non-governmental actor. Many in the government, private sector, and national security community believe that Russia is behind the hack. One major reason for this is the sophistication of the attack-such a sophisticated attack, including malware and IP addresses never before used in an attack cyberattack, and the knowledge/capability to launch the attack from US servers, indicates a state actor. The resources needed for such an attack point to the vast capabilities of a country, not an independent actor/group. This is bolstered by what was clearly a thorough understanding of Einstein's capabilities (and blindspots) and the American prohibition on the NSA and DHS accessing and protecting private servers.

As reported by Reuters in the immediate aftermath of the attack, many were already pointing to a nation-state being the culprit, due to the sophistication of the attack (Bing & Minn, 2020). David Sanger, a New York Times reporter who contributed to two of the articles cited in this report, was responsible for breaking the story of Operation Olympic Games, which detailed the United States (and Israel) uploading a worm into the digital infrastructure of an Iranian nuclear plant which allowed them to control the centrifuges used to enrich uranium and to manipulate the systems which monitored the centrifuges (Sanger, 2019). The Stuxnet worm eventually made its' way into the greater hacking community, where it was examined by cybersecurity experts (Sanger, 2019).

John Ward – Cyberblog December 2020

These experts were baffled by the sophistication of the worm, as it contained a number of "zero-day" components-components that have no precedent in any previous cybersecurity incidents (Sanger, 2019). These components take a significant amount of money and knowledge to develop. Furthermore, the worm had been designed to target very specific machinery and computer systems within the Iranian nuclear plant, indicating a significant amount of foreknowledge and research into the facility (Sanger, 2019). These factors led Mr. Sanger to suspect that a country was behind this attack, as it was extremely unlikely that any entity without the technical knowledge, money, development capabilities and espionage capabilities would be able to pull off such a sophisticated attack (Sanger, 2019). This theory, in tandem with the obvious political motives behind the attack, led Mr. Sanger to theorize it was the United States behind the attack-in this he was proven correct (Israel also played an important part) (Sanger, 2019).

There seems to be a significant amount of agreement that Russia's SVR is behind the SolarWinds attack. Senator Richard Blumenthal (D-Conn) tweeted that the Senate had received a "classified briefing on Russia's cyberattack…" (Nakashima & Timberg, 2020). In a radio interview on 12/29/2020, Secretary of State Mike Pompeo said "we can pretty clearly say it was the Russians" (Sanger & Perlroth, 2020). However, later that same day President Donald Trump stated publicly that he did not know it was the Russians and that it could have been China (Sanger & Perlroth, 2020). President Trump also downplayed the hack by suggesting via Twitter that there had possibly been a hack on voting machines responsible for his electoral defeat, of which there was no evidence (Sanger & Perlroth, 2020). Privately, an anonymous source to the New York Times indicated that the President was calling the hack a "hoax" and pressuring associates to "downplay its' existence" (Sanger & Perlroth, 2020). While one could make the case that the President is being prudent by not accusing another sovereign nation of a cyberattack without a full and thorough investigation being conducted, President Trump's distrust and public contradiction of the federal intelligence community, particularly in respect to Russian cyberattacks, has a precedent. In a 2016, when questioned about the possibility of Russian cyber influence playing a positive role in his presidential campaign, President Trump instead suggested that it could have been "the Chinese" or "a 400-pound person sitting on their bed" (Sanger & Perlroth, 2020). This was in direct contradiction to the findings of the national intelligence community, and 12 Russian nationals were eventually indicted for interfering with the 2016 elections (Sanger & Perlroth, 2020).

John Ward – Cyberblog December 2020

This flippancy from the President of the United States is dangerous, both for the immediate threat of a Russian cyber threat, but also for the cybersecurity posturing of the nation moving forward. Without a clear understanding of who is responsible for a major cyberattack on the nation, the American public may find the issue too complex and intangible to focus on as a primary threat to the nation. Furthermore, the President's frequent public contradiction of his intelligence community, with seemingly no alternative theory beyond "maybe it was (x)" , demonstrate a significant lack of cohesion and purpose between those who are entrusted to monitor and combat external threats. Directly contradicting his own Secretary of State sends a confusing and dispiriting message to the American public, and emboldens potential perpetrators. This is especially troubling due to the fact that President Trump was provably mistaken with a similar set of circumstances in 2016.

It is unknown just how vast the SolarWinds hack was, and how many entities were affected. In the weeks subsequent to the initial disclosure, the amount of entities affected ballooned to an alarming number, and the true number may never be known. Nor will the ultimate goal of the attack, how successful it was, and exactly what was accessed. Within the federal government, officials are stating publicly that they don't think the Russians were able to access any classified material, but privately do not have a clear picture of exactly what was accessed (Sanger, Perlroth & Barnes, 2021). Even if Russia were unable to access classified material, they would have access to important national security documents. For instance, they may have had access to Black Start, the Federal Energy Regulatory Commission's plan for how the US would react in the face of a catastrophic blackout (Sanger, Perlroth & Barnes, 2021). This information is not technically classified, and Russia has been known to have implanted malware in the US power grid, and to have digitally caused a blackout in the Ukraine in 2015 (Sanger, Perlroth & Barnes, 2021).

Brad Smith, the president of Microsoft, likens the current national cybersecurity situation to the immediate post 9-11 federal intelligence situation-there is not a mandated structure for sharing information and too many agencies are sitting on the information they have, diminishing the chance to create a clear picture of the overall threat and to create actionable intelligence (Smith, 2020). In fact, Mr. Smith states that under current governmental contracts, companies like Microsoft and FireEye are legally prohibited from sharing information of breaches in parts of the federal government with other parts of the federal government (Smith, 2020).

John Ward – Cyberblog December 2020

Mr. Smith believes that this type of attack could become a "permanent part of the threat landscape" (Sanger, Perlroth & Barnes, 2021), and could in fact lead to a proliferation of sophisticated cyber attack capabilities, not only by the "limited number of governments that can invest in the invest in the talent needed to attack with this level of sophistication" (Sanger, Perlroth & Barnes, 2021), but also by the evolving threat of private companies and cyber "mercenaries" who are able to wield the tools developed by these nation-states to "blur the lines of culpability" (Sanger, Perlroth & Barnes, 2021).

Mr. Smith suggests that cybersecurity requires a unique approach of collaboration between the public and private sector (Smith, 2020). It is important to note that it was a private company, FireEye, that discovered the breach and private companies such as Microsoft, FireEye, and GoDaddy have coordinated the response (Newman, Lily H., 2020). It is largely through the vigilance and largesse of private companies that the intrusion is known in the first place, and is being combatted today. Senator Mark Warner (D-Virginia) said "…and if FireEye had not come forward I'm not sure we would be fully aware of it to this day" (Newman, Lily H., 2020). FireEye suffered an 8% stock drop in the immediate aftermath of disclosing the intrusion-it is naïve to think other private companies would react in the same way given the circumstances without being compelled to. Mr. Smith stated that many federal agencies were turning to Microsoft in the wake of the hack for information and guidance, showing a significant reliance on private entities and a lack of capability in the public sector (Sanger, Perlroth & Barnes, 2021).

The SolarWinds hack and response has raised significant issues on every level. Countless private entities and important federal governmental departments were using software that the majority were not even aware they were using-even fewer knew that the company had outsourced their engineering to Eastern Europe (Sanger, Perlroth & Barnes, 2021). A 2018 Government Accountability Office report found that "network monitoring by individual (federal) agencies is spotty" (Nakashima & Timberg, 2020), finding that "five were not persistently monitoring inbound or outbound direct connections to outbound entities" (Nakashima & Timberg, 2020), with many others only monitoring either inbound or outbound. The developer of this software, SolarWinds, had made only token efforts at security, a fact which would have been easily observed by any client taking the time to research them. Nor were they compelled to add any significant security measures, except by foreign legislation. Myriad federal agencies were reliant on the same of software, meaning that in the event of a breach (which did occur), they were all susceptible to the threat.

John Ward – Cyberblog December 2020

The government did not have sufficient means and/or the inclination to effectively deal with the situation, instead relying on private industry, who were by no means mandated to assist. The multi-billion dollar cyberthreat detection system deployed and monitored by the NSA was unable to identify the breach, and its' shortcomings have been identified for all the world to see and potentially exploit. The highest levels of government are engaged in a public show of distrust and contradiction, unable (or unwilling) to conclusively assign blame. It will be up to the Biden administration to examine the SolarWinds hack and chart a new course forward for the nation's cybersecurity policy. The nature of cyber threat is constantly evolving and augmenting, but in some respects the United States is lucky to have discovered the breach, as catastrophic as it was. The SolarWinds hack can act as a turning point for cybersecurity in the United States.

One final factor to consider is the opaqueness with which the United States acts in terms of their offensive cyber operations. The United States has run many similar attacks against foreign nations in the past, such as the previously mentioned "Stuxnet" and many against North Korea (Sanger & Perlroth, 2020). In David Sanger's book The Perfect Weapon, chronicling his investigation into the development of Stuxnet and its' deployment in Operation Olympic games, Mr. Sanger posits that the American people are kept ignorant of the America's offensive cyber actions against other countries (Sanger, 2019). It was many years after Operation Olympic Games was successful that it became public knowledge-without some eagle-eyed cybersecurity experts and effective investigative reporting, it may very well have never been known. Operation Olympic games occurred over a decade ago-if the US had that level of sophistication and the capability to upload it into a sovereign nation's infrastructure back then, there is no telling what they are capable of doing now, nor what they have done and are doing. Espionage and sabotage is an accepted part of international coexistence-in many cases, it would be naïve and self-defeating to inform the general public of these actions, even in a democracy. Cyberattacks exist in a unique place in international relations-never (to this point), crossing the threshold to an act of war, but with the capability to be tremendously destructive. It is unknown how many of the cyberactions against the United States are retaliations for offensive actions that the United States has taken-by design the doctrine of "defending forward" includes hacking into other countries' digital infrastructure.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog December 2020

Bombings, invasions and other military actions are generally subject to congressional approval, where elected representatives of the American people decide on the wisdom, legitimacy and consequences of such an action, while the American people witness the process. This public process largely does not exist for espionage and sabotage, because by their very nature they are secretive. In the United States, offensive cyber operations fall under this category, but perhaps that is creating a larger problem. The United States is more than likely participating, if not one of the leading parties, in the proliferation of offensive cyber weapons and cyber tools. This has significant ramifications- a populace believing that they are being victimized without cause by foreign nations can lead to aggression and mistrust. Significant cyber intrusions without a clear cause or retaliation can lead to the general population feeling weak and victimized, and may cause them to lose faith in their government's capabilities to protect them. There is a case to be made for the government being more transparent with their offensive cyber operations, and for the American people to get a clearer picture of their government's role in the proliferation of an international cyber arsenal.