[Top Secret]

BRIEFING MEMO

THE WHITE HOUSE

Washington

April 21, 2021

MEMORANDUM FOR JAKE SULLIVAN

FROM: Austin Kent, David Chen, Tanpong Tanthien, Mohammad Zaid Khaishagi

SUBJECT: U.S. response options against Russia regarding SolarWinds attack

Executive Summary:

This memorandum provides updates on the SolarWinds cyberattack ("SolarWinds") discovered in December 2020. It discusses the details of the attack and its effects on the U.S. government. To effectively evaluate potential response to the attack, this memorandum outlines the three key considerations: risk of escalation, effectiveness of deterrence, and alignment with doctrine for cyber-offense by General Nakasone.

The memorandum also presents three response options, which are currently under consideration. The probability of success for each response is determined to be at least even, according to National Intelligence. All three responses are evaluated under the three key considerations previously outlined. The memorandum concludes with the recommended response option considering the relative benefits and drawbacks of each option.

The response options being considered are: (1) infiltrating and inserting a deterrent message into Russia's Main Intelligence Directorate (GRU) systems; (2) damaging the operations of the oil and gas company Surgutneftegas, owned at least 37% by Russian President Vladimir Putin; and (3) causing a day-time blackout during the summer in the Russian city of Akademgorodok, known as the "Russian Silicon Valley."

The option we recommend is (1) infiltrating and inserting a deterrent message into GRU systems. This option has the least likelihood of escalating conflict between the U.S. and Russia by avoiding provocative actions while simultaneously demonstrating U.S. strength to respond to any hostile actions that Russia undertakes. It also increases the likelihood of Russia pursuing a diplomatic resolution by conveying the intended message and minimizing Russian arguments for counter-offensives. Such an approach increases the effectiveness of deterring Russia from conducting kinetic attacks. However, Russia may still retaliate by launching more aggressive cyber attacks. This option is in agreement with the announced

cybersecurity doctrine of pursuing forward defense and a persistence strategy by establishing a presence in GRU networks and systems.

Background:

On December 13, 2020 (Sunday), FireEye detected a cyber intrusion that leveraged Orion, a network-monitoring tool developed by SolarWinds. The attackers inserted malicious code into Orion software updates to spy on the U.S. government and private companies. Over 18,000 SolarWinds customers were at risk [1]. According to National Intelligence, it is "almost certain" that the GRU was responsible for the attack. Moreover, it is "probable" that Vladimir Putin authorized this attack. The harms caused to the U.S. government are as follows:

1. The indiscriminate nature of the espionage poses a threat to national security and public safety. Many U.S. agencies including the Department of Homeland Security, National Nuclear Security Administration, and Treasury were attacked. This intrusion also placed a heavy financial burden on the government and the private sector.

2. Russian past behaviour raises the risk that the intrusion is a possible setup for larger attacks. The GRU could destroy, alter data, impersonate legitimate people and blackmail the CIA and NSA to recruit spies. The market data stolen could be used to manipulate the U.S. economy [2].

3. This attack is part of Russia's persistent effort to undermine U.S. democracy. The GRU realizes that U.S. law prohibits intelligence agencies from monitoring private systems based in the U.S., so they are exploiting our democratic legal restriction to their advantage.

4. U.S. Cyber Command, which receives billions of dollars in funding, failed to protect American networks and thus faces reputational damages. Instead, a private company was first to discover the breach [1].

Discussion:

Key Considerations:

- Avoiding Escalation

  The primary goal of any response should be to demonstrate the capability and willingness of the U.S. to engage Russia, while de-escalating hostilities. So, an evaluation of the probability of escalation is warranted. The current amassing of Russian troops near Ukraine's border contributes to the volatility of the

conflict and makes any U.S. response riskier in terms of escalation. [3] Furthermore, violating any international humanitarian laws would give Russia justification for retaliation. Minimizing the risk of escalation through a response that does not exceed Russia's actions would be advisable.

- Deterrence

  Our second criteria for evaluation is based on the deterrence these attacks would provide against Russia. The attack we choose to carry out should send a clear message on why we have taken retaliatory action. The attacks should be assessed in accordance with the current Russian political climate in determining their deterrence. The attack should convey the U.S.' capability and willingness to respond to future attacks [4].

- Alignment with Announced Doctrine

  Our third criterion for evaluation is based upon General Nakasone's doctrine for cyber offense. The attack we select should have a persistent presence in the Russian systems. The attack should create a forward defense for the United States cyberspace and seek to engage the enemy in their networks [5].

Response options:

The three following options are under consideration with each being equally likely to succeed:

1. Inserting a message into GRU systems:

This response option involves infiltrating the GRU networks. We would insert a deterrent message into the workstations of the GRU: "Desist within 14 days from all actions to exploit the SolarWinds vulnerabilities, or we will take serious, kinetic action against the Russian government."

2. Attack on Surgutneftegas oil Refinery:

For this response, we would disrupt the operations of an oil company, Surgutneftegas, owned approximately 37% by Vladimir Putin. Once this is achieved, diplomatic communication claiming it in response to SolarWinds would be sent to Russia.

3. Day-time blackout in Akademgorodok:

This option would be aimed at infiltrating the electricity grid of Akademgorodok, known as the "Russian Silicon Valley," followed by causing a day-time blackout during the summer. A

diplomatic communication would be sent to Russia claiming the attack in response to SolarWinds.

Analysis:

1. Inserting a message into GRU systems

The most significant benefit of this option is avoiding escalation. In this approach, the U.S. would be able to convey its strength in a way that gives Russia little grounds to pursue overt retaliation. Inserting a message directly into GRU systems ensures that any **evidence of our actions cannot be publicized by Russia to gather international support for retaliation.** Since **overt retaliation becomes difficult for Russia**, it is likely to **lead to a diplomatic resolution**. Additionally, by giving Russia the option to **de-escalate the situation without being perceived as weak**, it is effective for avoiding escalation and improving deterrence.

The approach would be effective for the purpose of deterrence as it **demonstrates U.S. cyber capabilities** by intruding into the Russian systems [6], while **not damaging any infrastructure** and **keeping the conflict in the same domain**. It gives Russia an **opportunity to withdraw without being provocative.**

Furthermore, since the approach **establishes a presence on GRU systems**, it follows General Nakasone's doctrine which advocates pursuing **forward defense** by engaging the enemy in their own networks and following a **persistence strategy.**

However, even though Russian justification for overt retaliation may be minimized, it may still **invite retaliation and stronger attacks in the realm of cyberspace**. This would be a serious threat, particularly considering the **presence established through SolarWinds.** Additionally, in light of current **tensions with Russia along the Ukrainian border,** an intrusion into their governmental systems may be **seen as firing the first shot.** Moreover, the U.S. response may also be **perceived as weak** since no damage is ultimately caused.

2. Attack on Surgutneftegas oil Refinery:

This response provides many advantages for deterrence. **Attacking Putin's personal finances encourages him to reconsider launching attacks** on the U.S. Moreover, this response also **sets an example for Russian oligarchs that continuing to financially support Putin's hostilities towards the U.S. will lead to personal financial losses** [7]. Following the forward defense strategy proposed by General Nakasone, an attack on the oil refinery would be a step towards achieving immediate responses and **imposing costs on adversaries** of the U.S. [5].

By attacking the Surgutneftegas oil refinery, the U.S. is escalating the conflict. This could lead to similar attacks from Russia against U.S. oil companies. Since the **U.S. refused**

Putin's cyber ceasefire treaties prior to SolarWinds, it could be used by Russia to justify further retaliation [8]. Depending on the significance of the oil refinery attack, the United States may damage its own reputation without having a significant financial impact on Putin. Also, it is **only "probable" that Putin was responsible for SolarWinds**, so this may be viewed as unprovoked aggression. Lastly, since there are U.S. pension funds (Blackrock, Vanguard) in the oil company, it **entangles the U.S., thus attacking it may harm our citizens** [9].

3. Day-time blackout in Akademgorodok:

The key advantages of this option are mainly regarding deterrence and doctrine. A day-time blackout in Akademgorodok will **demonstrate U.S. cybersecurity capabilities to retaliate** against Russia and deter other nations from similar activities. Furthermore, it will **undermine Russian citizens' faith in their government's** cybersecurity capabilities and put pressure on the Russian government to expect future damages if they escalate the conflict. Lastly, this response aligns with the **forward defense strategy** because strategic advantages in cyberspace stem from the "use and not the mere possession of cyber capabilities [5]."

Nevertheless, the drawbacks of causing a day-time blackout far outweigh any benefits. First, this indiscriminate response could harm innocent civilians who are not responsible for the ongoing conflict between the U.S. and Russia. Large-scale **cyber attacks on civilians can lead to danger and even death in severe cases** [10]. Second, since the **harm of SolarWinds is restricted to espionage, such a response can be seen as aggressive**. Furthermore, **Russia used the same blackout measure against Ukraine** during the Crimean annexation [11]. Russia could interpret the U.S. power outage response as an **invitation for war.** Lastly, Akademgorodok is considered to be the 'democratic oasis' of Russia [12]. The U.S. should **not alienate people with similar beliefs in Democracy.**

Recommendation:

From the analysis of the three responses, we recommend option (1): Inserting a message into GRU systems. This course of action will demonstrate U.S. cyber capabilities and a willingness to take action against Russia. Further, it does not involve civilians and only targets the Russian government. It dissuades Russia from pursuing escalation and encourages a diplomatic resolution. The other options are riskier for escalation, especially option (3) which mirrors Russia's actions during the Crimean annexation, leading them to expect similar simultaneous military action on the Ukraine front.

Though the other options may be more effective for the purpose of deterrence, those approaches may not yield the most desirable result. Attempting to achieve deterrence by damaging their infrastructure, while both nations are in a mutually provocative position militarily, has the possibility of triggering armed conflict, which undermines deterrence.

The recommended option achieves forward defense and persistence strategy, in line with General Naksone’s doctrine for cyber defense.

References

[1] I. Jibilian, “The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal,” Business Insider, 15-Apr-2021. [Online]. Available: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12. [Accessed: 16-Apr-2021].

[2] Guardian Staff and Agency, “Deep US institutional secrets may have been exposed in hack blamed on Russia,” Yahoo! Finance, 16-Dec-2020. [Online]. Available: https://finance.yahoo.com/news/deep-us-institutional-secrets-may-215139085.html. [Accessed: 14-Apr-2021].

[3] A. Odynova, “Russia warns U.S. to stay away for its ‘own good’ as Ukraine standoff intensifies,” CBS News, 14-Apr-2021. [Online]. Available: https://www.cbsnews.com/news/russia-ukraine-united-states-standoff-fears/. [Accessed: 22-Apr-2021].

[4] T. M. McKenzie, “Is Cyber Deterrence Possible.” Air Force Research Institute, Maxwell Air Force Base, Jan-2017.

[5] W. T. Eliason, “Defending Forward.” Joint Force Quarterly, 2019.

[6] J. S. Nye, “Deterrence and Dissuasion in Cyberspace.” MIT Press Journals.

[7] S. Baker, “Four principles to guide the US response to cyberattacks,” Fifth Domain, 07-Feb-2019. [Online]. Available: https://www.fifthdomain.com/thought-leadership/2019/02/07/four-principles-to-guide-the-us-response-to-cyberattacks/. [Accessed: 17-Apr-2021].

[8] A. Troianovski and D. E. Sanger, “Putin Wants a Truce in Cyberspace - While Denying Russian Interference,” The New York Times, 25-Sep-2020. [Online]. Available: https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html. [Accessed: 16-Apr-2021].

[9] “SURGUTNEFTEGAS : Shareholders Board Members Managers and Company Profile: RU0008926258: MarketScreener,” MarketScreener.com | stock exchange quotes| Company News, Apr-2021. [Online]. Available: https://www.marketscreener.com/quote/stock/SURGUTNEFTEGAS-6491739/company/. [Accessed: 22-Apr-2021].

[10] W. Ralston, “The untold story of a cyberattack, a hospital and a dying woman,” WIRED UK, 11-Nov-2020. [Online]. Available: https://www.wired.co.uk/article/ransomware-hospital-death-germany. [Accessed: 22-Apr-2021].

[11] N. Wojtowicz, “Strategic significance of the Crimean annexation.” Panorama, 01-Jan-2015.

[12] The remote 'democratic' oasis of Soviet Russia. BBC, 2019.