SOCIAL SCIENCE REVIEW ARCHIVES
ISSN Online: 3006-4708
ISSN Print: 3006-4694
https://policyjournalofms.com

State, Surveillance, and Cyberspace: An Intelligence Analysis of Operation Aurora

Fatima Nasir [1], Rabia Sohail [2]

[1,2] Department of Political Science and International Relations, University of Management and Technology, Lahore Email: s2022188020@umt.edu.pk s2022188019@umt.edu.pk

DOI: https://doi.org/10.70670/sra.v3i2.789

Abstract

The fact that Operation Aurora happened and was most likely undertaken by Chinese state-connected actors, introduced major changes to the way global cybersecurity works. The operation which was active from late 2009, went after more than 20 big American companies, including Google and Adobe, as well as Chinese human rights activists and dissidents. This paper looks at how Operation Aurora worked, why it was done and what cybersecurity lessons were drawn from it, all in the context of national security, relations between countries and cybersecurity at a global scale. Through the case study methodology and combining theories of realism and securitization, this analyses shows how cyber operations are used as means of power and control of ideas. According to the paper, Operation Aurora reached its main intelligence objectives, but at the same time changed how cyber deterrence, digital sovereignty and cyber security intelligence were discussed afterwards.

Introduction

Operation Aurora was a sophisticated cyber operation launched by state-sponsored actors attributed with China in 2009, targeting over twenty US-based firms and companies like Google, Adobe, Juniper Networks, Northrop Grumman etc. along with the Gmail accounts of Chinese journalists, human rights activists and dissidents. The cyber intrusion of systems initiated on the day of Christmas, an official holiday in the United States, thereby providing lesser security parameters in otherwise highly secured systems because of the skeleton crews. It was initially disclosed by Google in January of 2010 with other companies affirming the claims made by Google. This attack remains significant in the history of cyber operations as it expanded the spectrum of referent objects in cyber operations from CNII related to defense and confidential state information to private firms as well. Operation Aurora was a turning point in cyber intelligence history, marking the beginning of nation-state-sponsored attacks against not merely data, but strategic geopolitical targets. The ultimate objective of the attack went beyond corporate espionage. It seemed to comprise attempts at finding individuals targeted by U.S. intelligence—invoking serious question regarding counter-surveillance practices, geopolitical tensions, and security of critical information infrastructures.

Literature Review

Debate in the academic world about cyber warfare and cyber espionage sponsored by states has grown a lot over the past decade. Experts say that this operation changed the way people view cyber warfare and safety of nations. Based on research by Rid and Buchanan (2015), hiding the source of cyber-attacks and setting wider political or strategic goals are now core characteristics

of cyber warfare. This is consistent with the secret approach of Operation Aurora which depended on using zero-day bugs and advanced persistent threats (APTs) to secretly invade strongly protected networks.

Such studies as the one conducted by Chen, Desmet and Huygens (2014) state that APTs stand for the new approach of conducting long espionage operations to obtain useful business and intelligence data. The Hydraq Trojan and using CVE-2010-0249 in the Internet Explorer showed this change in methods and motivation.

In opposition to traditional views, Valeriano and Maness (2015) argue that cyber strategies are (first and foremost) applied for influence building and power display, rather than for actual fighting. The attack was intended to give China power over information and dispute the West's technological leadership which is what China started with Operation Aurora. Lindsay (2015) and Segal (2018) mention that China involves different organizations and groups in conducting cyber campaigns, sometimes for defense and sometimes for attack, just like Shanghai Jiao Tong University and PLA Unit 61398 have been identified with.

Research Gap

While Operation Aurora is extensively studied by the cybersecurity community addressing and analyzing the technical dimensions of the operation identifying the backdoors, exploits, trojans, cyber tools employed without fully integrating the intelligence rationale, the potential strategic objectives and motivations, stakeholders and pre-operational intelligence measures that served as the underpinnings of this campaign. Moreover, much of the scholarly literature discusses Operation Aurora limited to the corporate sector cybersecurity dynamics and the consequent geopolitical implications of such actions while analyzing the role of intelligence agencies and state-sponsored cyber campaigns and private firms work in a synergy. Not enough research has looked closely at the links between national interests, roles taken by participants and intelligence duties before state-sponsored cyber espionage begins. By studying Operation Aurora, this study focuses on how China intended the operation to work, who participated, the intelligence gathering methods used and how much it achieved for China's national security. Because of this, it helps people understand that behind cyber operations lies politics and the role of intelligence more than just technology.

Research Questions

1. What were the stakeholders involved in this intelligence operation?
2. What were the national security objectives and concerns that formulated the underpinnings of this operation?
3. How were intelligence measures identified and adopted that eventually led to the conduction of the Operation Aurora?
4. Was Operation Aurora able to achieve the predetermined interests and objectives of national security?

Methodology

Through the use of a qualitative, interpretivist case study, this research looks at Operation Aurora using ideas from cybersecurity analysis, international relations and intelligence studies. Data is obtained mainly from cybersecurity firm investigations such as those by McAfee, Crowd Strike and Symantec; open-source intelligence (OSINT); and from policy documents by well-known think tanks including the Council on Foreign Relations and the Harvard Belfer Center. Secondary academic sources give you the background ideas and explanations. Through process tracing, it is possible to find out the events and decisions that brought about the operation from its very start to disclosure. There are very few numbers available because the operation is covert, so the study instead presents an in-depth summary based on experts' findings and careful analysis. An analysis

method is chosen, reviewing the aspects of the attack, from tactical (technically) to operational (based on intelligence) and to strategic (geopolitical) ones.

Theoretical Framework

The motivation and outcomes of Operation Aurora are studied using realism and securitization theory which give the study a two-sided view.

Those who believe in realism say that states think and act sensibly in a global system without rules, where the focus is on gaining power and remaining alive. Cyber capabilities, with this approach, help countries win in strategy, shield important interests and handle perceived dangers. The attack of Operation Aurora is a clear example of China's strategy to become self-sufficient in technology, secure from threats and powerful on the world stage, by taking source code and surveillance data from U.S. companies (Nye, 2010).

According to Buzan, Wæver and de Wilde's securitization theory (1998), security matters are shaped through the way people speak and write about them. An issue like state ideology or regime survival is considered existentially dangerous when politicians treat it as such which justifies taking actions that do not have to follow proper procedures. Because of Operation Aurora, China saw its information sovereignty and ideological rules as major national interests, allowing secret cyber actions taken against both Google and political opponents.

These theories point out that cyber operations protect both a country's physical security (realism) and its ideological image (securitization). This way of looking at it reveals that Operation Aurora was strategic, not only a technical advance and occurred within the context of power and ideology within the digital world.

Stakeholders and Intelligence Agencies Involved

After the disclosure by Google in a blog and multiple other firms, McAfee, a US-based cybersecurity firm led the investigation and the attribution of Operation Aurora and provided security patches and relevant information to the public. Additionally, National Security Agency, Federal Bureau of Investigation, Microsoft and other affected companies contributed to the investigation of the said operation. The investigation on the attack vectors revealed the origin of the operation to be in two schools in China i.e., Shanghai Jiao Tong University and Lanxiang Vocational School. The schools appear fully-functional but are suspected to be covers for chinese cyber The source file for the attack identified was named as AURORA, which was later designated as the appellation for the operation. Based on the gathered evidence, the United States accused China for attempts of breaching the security of data and intellectual theft of source codes of major firms like Google.

Although China denied the responsibility of the operation, the evidences available indicate towards a deeper involvement of China. Analysis of the targets i.e., chinese human rights activists, chinese operatives in the United States and source codes of major commercial firms; the larget number of targets and the sophistication of the cyber tool deployed in the operation suggested the backing of the state considering the organization of all attacks launched on multiple firms simulatneously and resources utilized in the conduction of the operation. The attack is associated with Ministry of State Security responsible for both foreign intelligence and counter-intelligence known for coordinating with independent operators or contractors often refered to as cyber militia based in universites or shell companies which in this case explains the origin of attacks conducted to be in schools. Other involved actors include the chinese military cyber unit PLA Unit 61398 under the People's Liberation Army (PLA) General Staff Department known for using Advanced Persistent Threats (APTs). The independent investigations by companies revealed multiple names for the associated groups with the PLA Unit 61398. Symantec named the group as the Elderwood group based on the frequently used word in the code. CrowdStrike named it as Sneaky Panda while Del

refered to it as Beijing Group. For the pupose of consistency, the group would be refered to as the Elderwood here onwards in this document.

Modus Operandi

Prior to the initiation of the operation, a comprehensive intelligence reconnaissance was conducted, identifying the target companies and employees vulnerable to phishing. The companies targeted were meticulously shortlisted by the Elderwood group. The cyber tool used did not directly target the major defense and industrial firms for instance Lockheed Martin, Boeing, Raytheon and General Dynamics, rather they leveraged the intelligence acquired in preliminary reconnaissance and in some cases, by the study of the product they provided. After studying the product, the perpetrators employed reverse engineering, identifying the parts and materials used and their providers. The employees of provider companies, often with lesser secure systems, were targeted using spear-phishing and water holes. Once their cybersecurity was compromised, any online interaction via emails or other internet sources would result in access to the systems of firms and industries with high-security IT departments. This indirect method of approach rendered the security breach easier and complicated the attack vector (pathway of cyberattack), making it difficult to trace and identify the true perpetrator. Similar plan of action was adopted for gaining access of the systems of Chinese human rights activists by deploying watering hole technique on the websites frequented by those individuals.

The attack was initiated by exploiting a zero-day vulnerability in the Microsoft Internet Explorer (later identified as CVE-2010-0249) which served as a conduit for the Trojan Hydraq to intrude into the targeted systems. When a victim visited a site with the malicious code, it would exploit the zero-day in Internet Explorer and get latched on to the host system. In the host system the Hydraq trojan would be downloaded and executed. Once executed, Hydraq would automatically download additional files and, being a trojan, disguise itself a file of the Operating System of the device rendering it undetectable and persistent against any anti-malware software. When activated successfully it would establish a command-and-control communication with perpetrator system allowing it to execute commands, transfer files, steal credentials, scan internal systems for potential valuable information and data exfiltration on the host system. Hydraq masqueraded itself as an SSL, reassuring the victim of data encryption and its lateral movement across the networks provided attacking party access to adjacent systems and read mails and documents.

National Security Objectives and Concerns

The national security concerns, the resultant objectives and the rationale behind this risk and security assessment spread on a broad spectrum ranging from surveillance and counter intelligence to intellectual data theft. The root of the concerns lies in protection of the authoritative regime and its hold.

1. Information Sovereignty

In 2006, Google officially launched its local search engine google.cn following extensive negotiations with the Chinese authorities on the compulsions of government-imposed censorship. The requirements mandated by the Chinese government became more stringent leading to the Olympic games held in mainland China. The censorship of information resulted in friction between the founders and the Chinese authorities, leading to the shift of traffic to google.com.hk (Hong Kong) and then the eventual withdrawal of the search engine in 2010. The Communist Party of China is known to often prioritize regime protection over state protection. An uncensored search engine was perceived as a threat to the information sovereignty of the state that monitors and controls public dissent domestically as well as overseas. Chinese human rights activists, lawyers and journalists used foreign platforms that provided them encrypted communication. These

individuals could engage in anti-state or anti-CCP discourse and activities or lobby in international organizations without being monitored.

2. Technological Advancement

The withdrawal of foreign technology firms and software houses from mainland China likely created favourable conditions for the local firms and projects by providing them access to an expanded market with reduced foreign competition. The operation also targetted the source codes files of companies like Google, Adobe, Yahoo etc. The acquired source codes can be subjected to reverse engineering and utilized to accelerate the developement of local companies with comparable features available, shortening the route to innovation. This would reduce the reliance on the Western technologies which are viewed as vehicles for the transmission of western ideas and values in China potentially challenging the state's information control framework. It also aligns with China's "indigenous innovation" policy program—a program launched in the mid-2000s aimed at stimulating domestic technology capabilities by legal and covert means.

3. Counter Intelligence

Another key driver behind the operation Aurora was chinese counter-intelligence agenda. China, in part, sought to verify the suspicion of its spies and operatives being under the US surveillance. Following the intelligence failure in the 9/11 incident, US had ramped up its surveillance and intelligence gathering and centralized the intelligence oversight by establishing the Director of National Intelligence. If the Gmail accounts of the operatives were being court-order wiretapped by the US, China would have a compelling national security interest identifying the agents compromised. Contrary to the overarching aggressive posture in the operation, this reflects a defensive rationale from the Chinese government.

4. Rising Tensions between US and China

By 2009, tensions between US and China extended their competitiveness to the cyber domain. The United States had adopted a very critical stance on the Chinese Great FireWall, while China viewed US-based firms in China as the conduits of western ideology. Operation Aurora reasserted China's position regarding the foreign firms, reinforcing the idea that their presence in china is conditional and highly-surveilled.

Intelligence Measures and Data Collection Tools

Operation Aurora remains significant amongst all the prior cyber operations due to the nature of its target. To achieve the objectives outlined initially, multiple intelligence measures including intelligence reconnaissance and strategic intelligence gathering.

1. Cyber Reconnaissance

Cyber reconnaissance serves as a precursor to the broader cyber operations linked with data exfiltration and espionage. Operation Aurora required the identification of key individuals and vulnerable systems in the foreign firms to access the required confidential data and emails. A comprehensive record of all websites and webpages frequented by the targets was compiled, providing the information on potential sites that could act as watered hole. Open Source intelligence (OSINT) was gathered by the surveillance of social media, publicly available company records or white papers. The information on vulnerable employees, key executives and the human rights activists acquired was subjected to scrutiny. This allowed the Elderwood group to meticulously curate personalized phishing emails as per their frequented contact nodes and sites, leading to malware infections and credentional theft. This aided in the social engineering and the spear-phishing campaign. Human rights activists were found to have frequented on the online website of Amensity International (Hong Kong) and the International Institute for Counter

Terrorism. These website seemed legitimate to the vulnerable visitors, but in fact had been water holed to compromise the security and breach into their systems

2. **Zero Days**

Secondly, the exploitable zero-day vulnerability (CVE-2010-0249) in the commonly used software (Internet Explorer) was identified which later served as a pathway for the Hydraq malware to breach the security of the compromised systems without alarming the cybersecurity systems and anti-malware software. The Elderwood group had access to multiple exploits across various websites which were simultaneously targeted in the cyber campaign. The perpetrators could access multiple zero-days on the spot and continue to exploit new zero-days due to access to source code of the targeted websites. The source codes were obtained using Cyber Intelligence (CYBINT)

3. **Mapping of Digital Footprint**

Thirdly, the mapping of the digital footprint of Chinese human rights activists and operatives was done by attempts to access payloads of emails and correspondence via Gmail accounts. The confidentiality of the correspondence was breached by interception of the internet-based communication as the accounts were being wire tapped. The data collection was done using Signal Intelligence (SIGINT)

Outcomes

Google's public disclosure of the breach in January 2010 was a strategic blow to the operation, despite its early success. This brought significant public and governmental attention to state-sponsored cyber-attacks and broke with the custom of corporations being silent in cyber crises. A portion of Google's decision to make the assault public was a protest against the censorship and monitoring practices of the Chinese government, which disproportionately target dissidents. Google responded by redirecting traffic to its servers in Hong Kong and announcing that it will stop filtering its search results in China. As a result, Google essentially withdrew from mainland China, which was detrimental to both sides: Google lost access to a sizable market, and China lost a significant digital platform. Increased government and business investments in cybersecurity infrastructure, threat detection, and collaboration between public and private institutions were also a result of Operation Aurora's public disclosure. It led to the broad implementation of enhanced incident response procedures, advanced persistent threat (APT) tracking, and zero-day monitoring. The global cybersecurity scene was reshaped in part by Operation Aurora. It was one of the first well-known instances in which a nation-state—in this case, China—was publicly blamed for cyber espionage. The U.S. government did not formally attribute the assaults at the time, but cybersecurity companies like McAfee, Mandiant, and CrowdStrike were able to link them to organizations associated with the People's Liberation Army in China. The attack influenced doctrines and cyber diplomacy globally and helped formalize cybersecurity as a field of national security. It made the development of international standards for conduct in cyberspace more urgent and raised international scrutiny of China's cyber activities.

Did it serve Intelligence Purpose

In order to determine whether operation aurora was successful or not, the outcomes are needed to be analyzed keeping the national security objectives in view. The outcomes combined would define the status of the operation. The first security objective was to obtain source codes of major firms, of which China did eventually gain an access to. The second security objective was to exfiltrate the data from the mails of the Chinese human rights activists. And third objective was to pursue counterintelligence measures to verify the status of Chinese operatives in the United States.

Lastly, the operation sought to protect and propagate the Chinese ideology of centralized control and surveillance of information in opposition to the western ideologies.

4. Tactical Success

From a tactical and technical standpoint, operation aurora was an undoubted success. Deploying the tools of cyber intelligence, the elderwood group was successfully able to penetrate into the source code repositories of the victim firms, providing conduits for the Hydraq malware to penetrate into the systems and consequently move laterally across the network of systems the host system was connection to. Use of supply-chain approach in accessing the target allowed undetected and deep penetration making the attack vector long and complex. The use of Advanced Persistent Threats (APT) permitted the malware to stay deeply rooted and persistent in the compromised systems, providing stealth and sophistication to the cyber campaign.

Evidence show that the perpetrators were able to access into the source code repositories at Google and Adobe, along with the classified Google Surveillance Databases that were being utilized by the United States to monitor and surveil Chinese operatives and their covert operations in United States by court-mandated wire tappings. It was not merely a technical access but also provided them with high-value intelligence on US surveillance goals. It can be concluded that on the micro level of execution and data exfiltration, the operation met its immediate goals, showcasing China's cyber espionage capabilities.

5. Strategic Success?

Contrary to the tactical level, on the strategic level, The operation cannot be fully categorized as a strategic success or a failure. The state was able to assert its information sovereignty ideology and as an immediate response, escort google out of mainlaind china, but it fell short in maintaining the covert element of the operation. The intelligence operation sought to be covert, but the intersection of chinese intrusion and the US wire tapping of chinese operatives exposed the either side to the other. The penetration and attempts of third party access were detected by the US authorities. Secondly, the elderwood group was required to maintain a plausible deniability but the investigations by the firms and antimalware companies like McAfrr along with their national counterparts revealed the location, traced back the attack vectors to chinese APT groups, especially those linked with the PLA Unit 61398 and identified the trojan and malware deoplyed in the operation. Thirdly, no information is present regarding the utility of the intelligence gathered on the Chinese operatives. The extent to which this information proved to beneficial remains unclear, whether they were able to identify compromised agents and abort their missions or plug the leaks in the intelligence system

Conclusion

Operation Aurora represents a turning point in the development of state-sponsored cyber espionage and cyberwarfare. The operation's strategic exposure by Google in 2010 led to a worldwide reevaluation of cybersecurity, corporate responsibility, and national defense mechanisms in the digital domain, even though it achieved short-term tactical success by taking advantage of a zero-day vulnerability to exfiltrate sensitive intellectual property and surveillance data. In addition to exposing the weaknesses of even the most technologically sophisticated companies, the event brought to light the increasing complexity of hostile cyber operations, especially those associated with state actors such as China.

References

Alperovitch, D. (2010, January 14). Operation Aurora: Leading to other threats. McAfee. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-aurora-leading-to-other-threats/

Alperovitch, D. (2010, January 15). More details on Operation Aurora. McAfee. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/more-details-on-operation-aurora/

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Chen, T. M., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. Communications of the ACM, 57(11), 56–61. https://doi.org/10.1145/2658987

Clarke, J. (n.d.). Operation Aurora: Tips for thwarting zero-day attacks, unknown malware. TechTarget. https://www.techtarget.com/searchsecurity/tip/Operation-Aurora-Tips-for-thwarting-zero-day-attacks-unknown-malware

Council on Foreign Relations. (n.d.). Operation Aurora. https://www.cfr.org/cyber-operations/operation-aurora

Exabeam. (n.d.). Operation Aurora: 2010's major breach by Chinese hackers. https://www.exabeam.com/blog/infosec-trends/operation-aurora-2010s-major-breach-by-chinese-hackers/

Gellman, B., & Soltani, A. (2013, May 20). Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. The Washington Post. https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7–47. https://doi.org/10.1162/ISEC_a_00189

NetworkChuck. (2022, October 8). Operation Aurora: The 2010 cyber attack that changed Google forever [Video]. YouTube. https://www.youtube.com/watch?v=_cs0DNhQuxA

Nye, J. S. (2010). Cyber power. Harvard Kennedy School Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cyber-power

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Segal, A. (2018). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.

Secureworks. (2010, January 20). Operation Aurora: Clues in the code. https://www.secureworks.com/blog/research-20913

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.