Cyber warfare

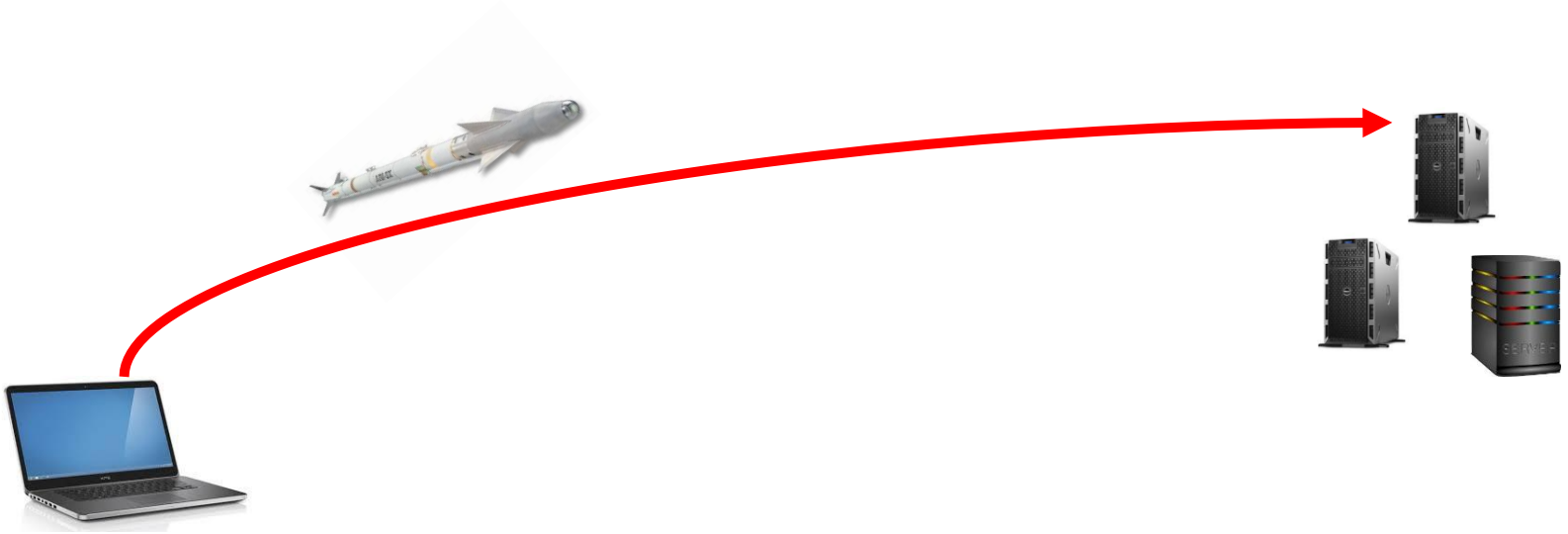
Cyberwarfare overview

Cyberwarfare is a fact of modern geopolitics and conflict. The most common weapon in cyberwarfare is weaponized malware. Cyber weapons development should be approached as an engineering task analogous to kinetic weapons engineering. Machine learning has been utilized in the defensive posture of cybersecurity, but there is a gap in the literature regarding the application of machine learning algorithms in the creation of weaponized malware for use by nation states in cyber conflicts. This paper explores methodologies for integrating machine learning in the engineering of weaponized malware. This current paper does not explore the coding machine algorithms into the malware, but rather describes the utilization of machine learning algorithms in the systems engineering development life cycle for creating cyber weapons.

What is it?

“Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.” – The RAND corporation

“In Cyberwarfare, Everyone Is a Combatant” – The Wall Street Journal https://www.wsj.com/articles/how-cyberwarfare-makes-cold-wars-hotter-1500811201



What is it?

“Faced with increased cyber attacks, US government is balancing attack on and defense from hackers and cyber criminals.”

“World War III is already here, and it's happening on the internet.”

-

http://www.aljazeera.com/indepth/features/2016/10/cyber-warfare-international-warfront-161020090216897.html

What is done?

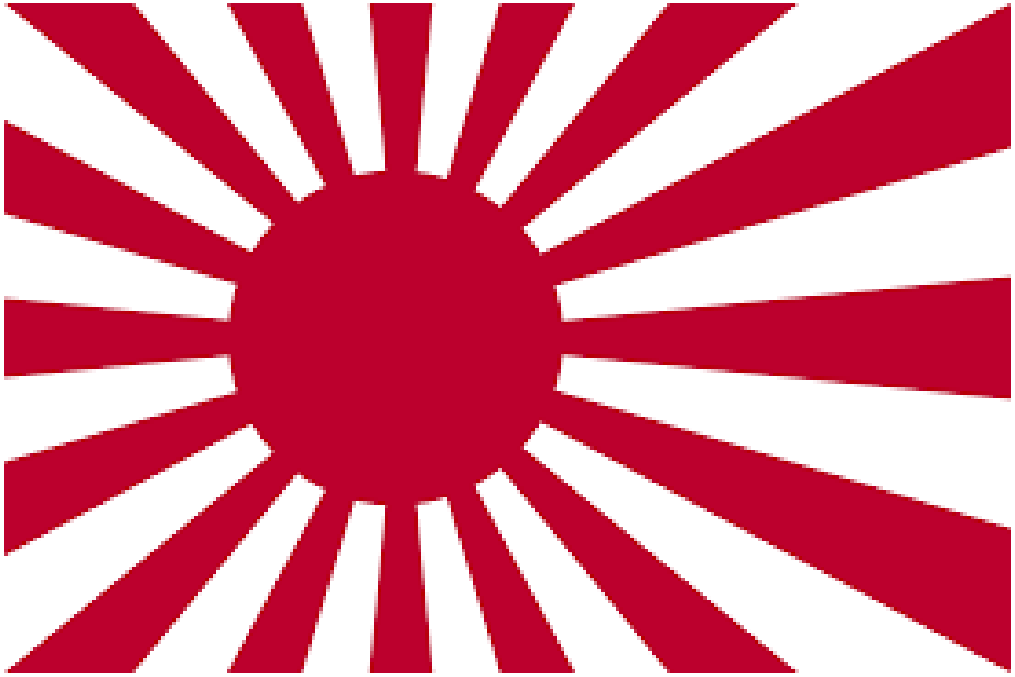
Sabotage

Warfare

Examples

Japan attacked by China

- Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was breached starting in October 2022 and continuing to June 2023. It is believed that the attack was executed by the Chinese military.
- - https://www.bitdefender.com/blog/hotforsecurity/japans-cybersecurity-agency-admits-it-was-hacked-for-months/



Canada being spied on

- Canada's electronic intelligence agency claims that APT group 31 has been targeting Canadian networks in 2024. The United States and the United Kingdome allege that APT31 is operated by the Chinese government.
- - https://www.cbc.ca/news/world/cyberespionage-china-hack-canada-targetted-1.7155482

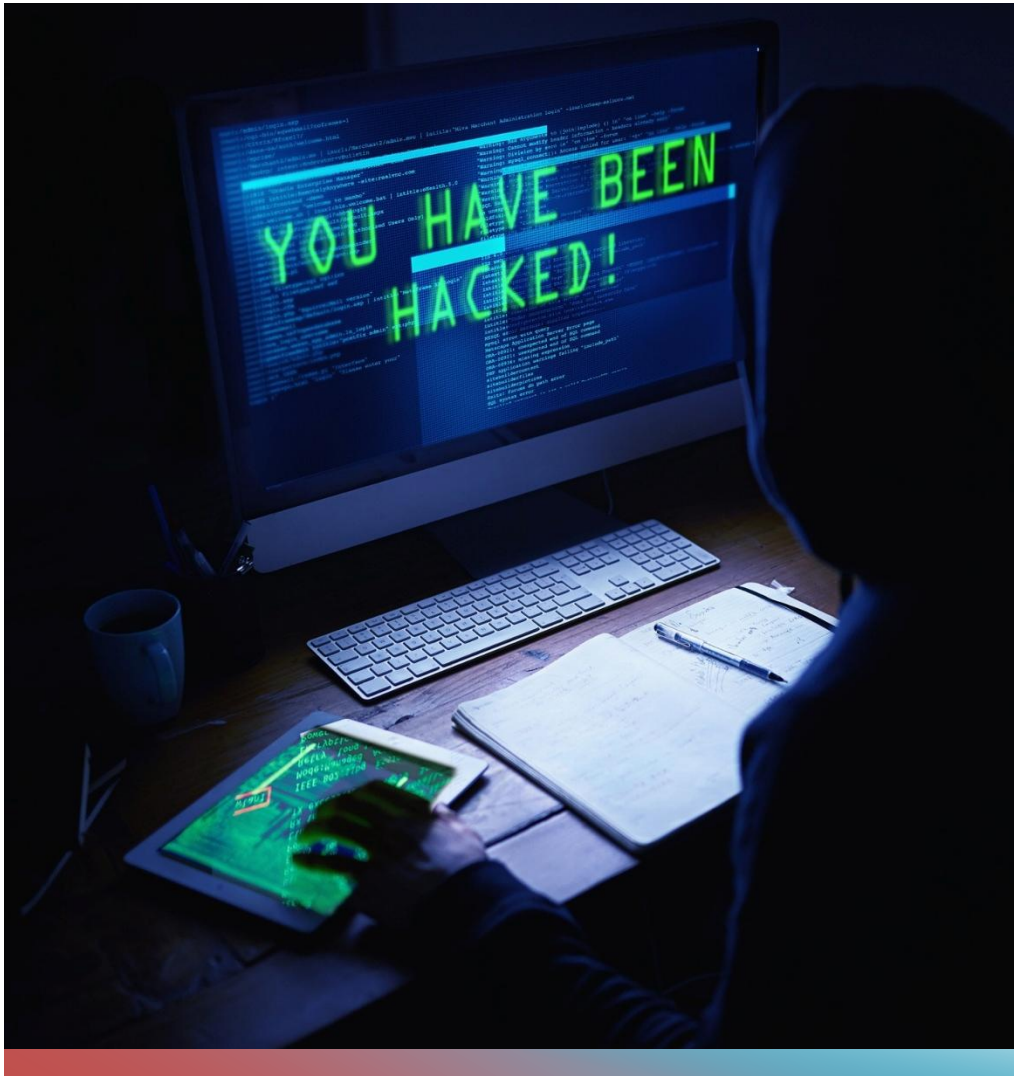
What is it?

Cyberattacks concurrent with Russia's invasion of Ukraine

https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare

https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do

https://news.harvard.edu/gazette/story/2022/02/harvard-cyber-expert-assesses-russia-threat/



US Removes Malware

2022 U.S. Claims it has removed malware around the world to prevent Russian cyber attacks. The Malware would allow GRU (Russian Military Intelligence) to create and control botnets.

US Attack on Russia

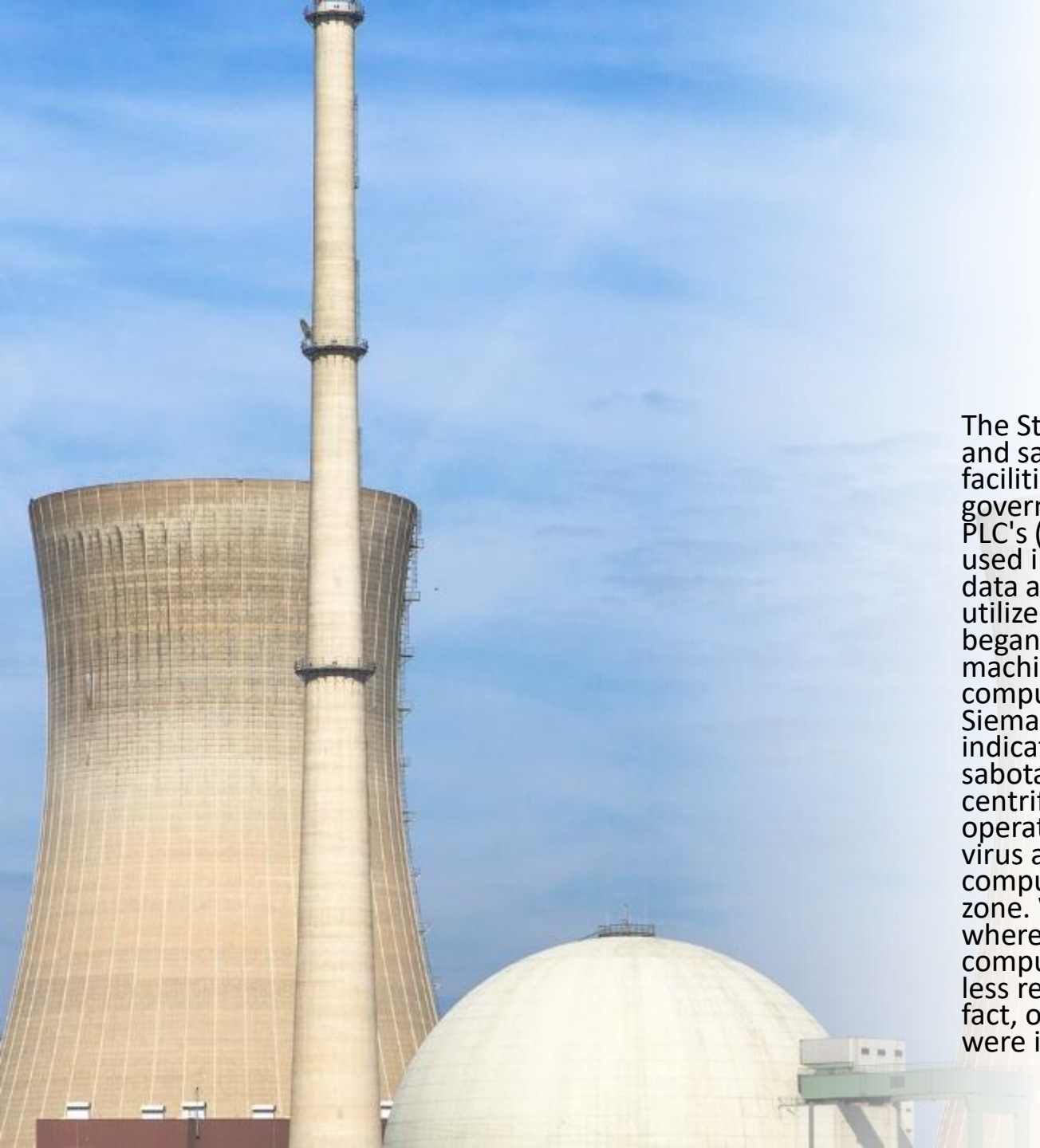
2019 Russia accuses US of planting malware on Russia's power grid.

https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html/

Iran attack on Turkey

2015 ½ of Turkey had a 12-hour power outage attributed to Iran. Attack was by APT group MuddyWater that has ties to Iran's Ministry of Intelligence and Security. They used malicious PDFs and Office documents as their main attack vector.

- https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/
- https://www.zdnet.com/article/state-sponsored-iranian-hackers-attack-turkish-govt-organizations/



Stuxnet

The Stuxnet virus was designed to infect and sabotage nuclear refinement facilities operated by the Iranian government. It specifically attacked the PLC's (programmable logic controllers) used in SCADA (supervisory control and data acquisition) systems. The software utilized four separate zero-day flaws and began by infecting Microsoft Windows machines and using those Windows computers as a launch point for attacking Siemans Step 7 software . Reports indicate that the malware successfully sabotaged 1/5th of Iran's nuclear centrifuges, making it a success from an operational viewpoint. However, the virus also infected and damaged computers outside of its intended target zone. While 58% of computers infected where in Iran, the remaining infected computers were not even Iranian, much less related to refining nuclear fuel. In fact, over 1.5% of infected computers were in the United States

Shamoon

The Shamoon virus was first discovered in 2012, and later a variant resurged in 2017 . Shamoon acts as spyware but deletes files after it has uploaded them to the attacker , June. The virus attacked Saudi Aramco workstations and a group named "Cutting Sword of Justice" claimed responsibility for the attack. A number of security officials within Saudi Aramco have blamed Iran for this attack. And, like Stuxnet, this virus infected systems other than the intended target.

Flame

The Flame virus is also a notable virus in the history of weaponized malware. This virus first appeared in 2012 and was targeting Windows operating systems. The first item that makes this virus notable is that it was specifically designed for espionage. It was first discovered in May 2012 at several locations, including Iranian government sites. Flame is spyware that can monitor network traffic and take screenshots of the infected system. The second item that makes this virus notable is that it used a compromised digital certificate to entice victim machines to trust the malware. Again, some sources identified the United States and/or Israel as the perpetrators.

THIS IS NOT NEW- OLDER INCIDENTS

- On 4 December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI)
- In December of 2009 Hackers broke into computer systems and stole secret defense plans of the United States and South Korea. Authorities speculated that North Korea was responsible. The information stolen included a summary of plans for military operations by South Korean and U.S. troops in case of war with North Korea, though the attacks traced back to a Chinese IP address.
- 2008 CENTCOM is infected with spyware. USB drive was left in the parking lot of a DoD facility. The worm was known as Agent.btz, a variant of the SillyFDC worm.
- 2009 Drone video feed is compromised

THIS IS NOT NEW- OLDER INCIDENTS

In 2009 a cyber-attack penetrated the U.S. electrical grid left software that would allow the attackers to disrupt power. The attacks came from China and Russia. The attacks were pervasive across the United States, affecting multiple power companies and regions. What is disturbing is most of these attacks were not discovered by the companies or their security departments, but rather by U.S. intelligence agencies

THIS IS NOT NEW- OLDER INCIDENTS

In 2016 Britain is using cyberwarfare against ISIS/Daesh http://www.bbc.com/news/uk-37721147

2016 Massive DDOS attacks against both US and Russian targets

2016 Iran begins seeking custom made malware and other cyberwar capabilities.

This is not new- older incidents Cyber terrorism -BlackEnergy

The BlackEnergy malware specifically affects power plants. The malware is a 32-bit Windows executable. BlackEnergy is versatile malware, able to initiate several different attack modalities . It can launch distributed denial of service (DDoS) attacks. It also can deliver KillDisk, a feature that would render a system unusable. In December 2015 a significant portion of the Ivano-Frankivsk region in Ukraine had no power for approximately 6 hours due to the BlackEnergy malware. The attacks have been attributed to a Russian cyber espionage group named Sandworm.

China’s APT

- The security firm, Mandiant tracked several APT's over a period of 7 years, all originating in China, specifically Shanghai and the Pudong region. These APT's where simply named APT1, APT2, etc.
- The attacks were linked to the UNIT 61398 of the China's Military. The Chinese government regards this units activities as classified, but it appears that offensive cyber warfare is one of its tasks. Just one of the APT's from this group compromised 141 companies in 20 different industries. APT1 was able to maintain access to victim networks for an average of 365 days, and in one case for 1,764 days. APT1 is responsible for stealing 6.5 terabytes of information from a single organization over a 10 month time frame.

Industrial targets

- May 2015 6 Chinese Nationals are arrested on charges of espionage and stealing intellectual property from U.S. Companies – Wall Street Journal
- CIO Magazine, examined the issue of government based cyber espionage in a 2009 article. Their article discusses the possibility that the Chinese government was behind a widespread infiltration of over 1200 computers owned by over 100 countries, with the express purpose of spying on the activities of those countries. The same article mentions that in 2007 the British government accused China of hacking into the systems of various British banks.

This is not new- older incidents

- During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with Denial of Service attacks by hacktivists (the name applied to individuals who work for their causes using cyber terrorism) protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as, “We won’t stop attacking until the war stops!” on U.S. government Web sites.

Rules of war

United States Defense Secretary Ashton B. Carter April 2015 announces a plan to discuss and examine the circumstances under which cyber weapons could be used against an attacker. – New York Times

Trends

DARK WEB MARKETS

WEAPONIZED MALWARE

MORE DIFFERENT GROUPS

Weaponized malware

- Flame and Stuxnet
- StopGeorgia.ru Malware
- FinFisher (spyware) released by WikiLeaks. Meant for Law Enforcement with a warrant.
- BlackEnergy Theoretically manipulate water and power systems including causing blackouts and water supply disruptions traced to Russian group ‘SandWorm’

Weaponized malware

- MiniPanzer and MegaPanzer variants of Bundestrojaner written by a Swiss government contractor and used to intercept skype over VoIP
- Duqu collection of malware related to Stuxnet. It has the prefix ~DQ on files, thus its name.
- Mahdi Malware reportedly used as spyware against middle eastern countries.

Private groups

- Anonymous declares war on ISIS
- Sandworm
- Russia v Georgia
- Middle East (Palestine, Israel, etc.)

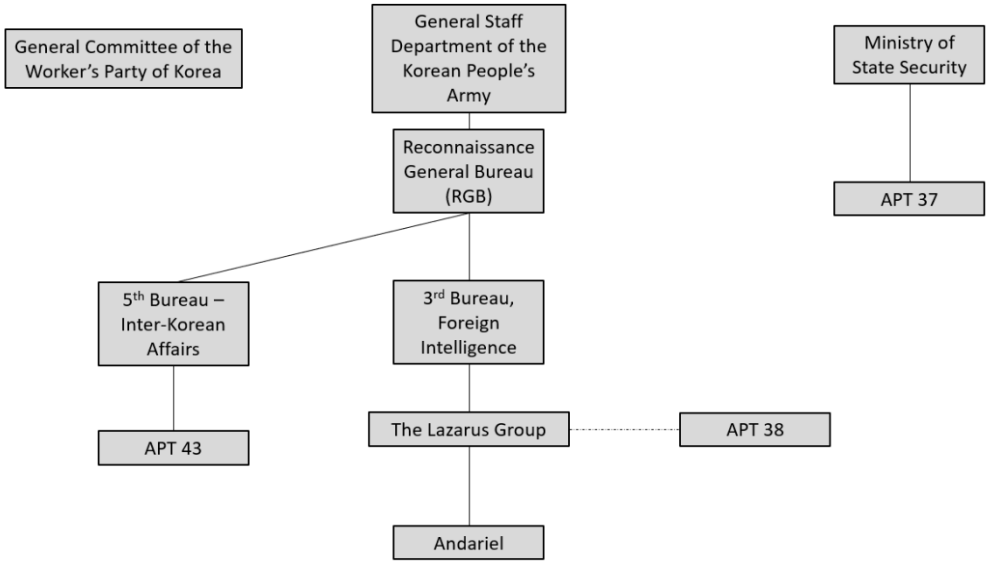
Cyber Terrorism

- Syrian Electronic Army attacked various media companies in August 2013 redirecting visitors to the company websites to sites the Syrian Electronic Army controlled.
- In 2015 the Federal Reserve Bank of St. Louis systems where breached redirecting users of its online research services to fake websites set up by the attackers.

Taxonomy for cyberwarfare

Stealth	Destructiveness	Monitoring
Level 1 malware operates like a traditional virus. It spreads aggressively and is quickly noticed on an infected computer.	Level 1 malware causes no damage to any part of the system. No files are deleted, system performance is not degraded in any way.	Level 1 malware does not monitor or capture any data.
Level 2 malware spreads aggressively but minimizes its impact on the target machine.	Level 2 malware does not delete any files nor directly damage the system, but its operation might degrade system performance.	Level 2 malware collects arbitrary data from a single source. This might be intermittent screenshots, as one example.
Level 3 malware spreads slowly, specifically attempting to avoid detection, and it minimizes its impact on the target machine. Level 3 malware also may utilize traditional techniques for avoiding anti-virus such as encrypting the payload, altering the virus signature, and similar techniques.	Level 3 malware does delete or encrypt certain key files, but otherwise leaves the infected machine operational.	Level 3 malware collects data from a specific application, or regarding a specific project. For example, a keylogger that only logs information typed into a specific application.
Level 4 malware uses selective targeting to only infect intended targets.	Level 4 malware renders the infected machine non-operational. Some firmware viruses are capable of this level of semi-permanent damage.	Level 4 malware collects a significant amount of data from the target machine. This includes screen capture and/or key logging along with harvesting emails, passwords, and searching for documents.
Level 5 malware utilizes all the techniques of level 4, then add to that advanced techniques such as self-destruction, virtual machine/sandbox detection, and the attack is launched from a source and location that is unlikely to be attributed to the actual threat actor.	Level 5 malware can cause damage outside of cyberspace. This can be accomplished via shutting down power grids, or other systems that could directly lead to loss of human life.	Level 5 malware essentially extracts a level of data from a machine that would be comparable to a digital forensics exam.

North Korea Cyber Threat



North Korean cyber-attack groups are controlled by the North Korean government. Therefore, it is not surprising that these attack groups operations overlap with the political goals of North Korea. Bernhart et al., (2023) published a chart of the organization control of North Korean cyber threat actor groups as of 2020 and a similar chart was published in 2022. Combining data from these charts with other relevant sources, the following composite chart was created:

North Korea Cyber Threat

Some sources use APT38 synonymously with The Lazarus Group; others consider APT38 a subgroup or a specialized unit within The Lazarus Group. The Lazarus Group is primarily focused on financially motivated cybercrime. It is known for large-scale financial heists targeting banks and financial institutions globally, using tactics such as fraudulent SWIFT transactions. One of the first operations attributed to APT38 was *Operation Troy* which took place from 2009 to 2012 and involved DDoS attacks on the South Korean government. APT38 is also alleged to have been behind a 2016 bank heist of 81 million (USD) from the Bangladesh Bank and 60 million (USD) from the Far Eastern International Bank of Taiwan

APT37

- APT37 is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. APT37 has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, and Golden Time. APT37 is also known as InkySquid, RedEyes, ScarCruft, Ruby Sleet, or reaper . APT37 has been associated with a number of attack campaigns. A sample of these will be described in the following paragraphs

APT43

- APT43, also known as the Kimsuky group (also known as Black Banshee) specializes in cyber espionage, particularly targeting individuals and organizations related to South Korean affairs, foreign policy, and international relations. This group is also referred to as Velvet Chollima. The word Chollima is a Korean word referring to a mythological flying horse. It should be noted that Velvet Chollima refers to APT43/Kimsuky, whereas Silent Chollima refers to Andariel threat actor group. After the Korean War, the country required rebuilding to function again. In order to expedite the construction, President Kim Il-sung devised the slogan "rush as the speed of chollima". Today, the Chollima in North Korea is synonymous with great speed and progress in the DPRK. It is not surprising to see the term Chollima throughout many North Korean threat actor groups.

China

Chinese cyberthreat actor groups—sometimes referred to as “Advanced Persistent Threat” (APT) groups—are state-linked or state-tolerated organizations that conduct cyber espionage, intellectual property theft, and occasionally disruptive operations. These groups typically operate under, or in alignment with, the strategic objectives of the Chinese government, particularly the People’s Liberation Army (PLA) and the Ministry of State Security (MSS).

China

- **APT1 (Comment Crew)**
  - **Affiliation:** PLA Unit 61398.
  - **Focus:** Long-term espionage against manufacturing, energy, and critical infrastructure.
  - **Notable Activity:** 2013 Mandiant report exposed them as a major IP theft actor.
- **APT3 (Buckeye / Gothic Panda)**
  - **Affiliation:** Linked to the MSS.
  - **Focus:** Aerospace, defense, energy.
  - **Notable Activity:** Associated with exploitation of “DoublePulsar” malware (before it was publicly leaked).
  - **APT10 (Stone Panda)**
- **Affiliation:** MSS.
  - **Focus:** Managed service providers (MSPs) to access multiple client networks.
  - **Notable Activity:** “Cloud Hopper” campaign (2014–2017).
- **APT27 (Emissary Panda)**
  - **Affiliation:** MSS.
  - **Focus:** Political and defense sectors, particularly in Asia.
  - **Notable Activity:** Targeting foreign embassies and defense contractors.
- **APT41 (Double Dragon)**
  - **Affiliation:** MSS contractors.
  - **Dual Role:** Espionage and financially motivated cybercrime.
  - **Notable Activity:** COVID-19 research targeting; software supply chain attacks.

China

- **Common Tactics, Techniques, and Procedures (TTPs)**
- **Initial Access**
  - Spear-phishing emails with malicious attachments.
  - Supply chain compromises.
  - Exploitation of unpatched public-facing applications.
- **Persistence & Evasion**
  - Web shells on compromised servers.
  - Living-off-the-land techniques (using built-in tools like PowerShell).
  - Custom malware families (e.g., PlugX, ShadowPad).
- **Data Exfiltration**
  - Compression and encryption before transfer.
  - Using legitimate cloud services (e.g., Dropbox) as staging points.
- **Operational Security**
  - Use of compromised third-party infrastructure.
  - Regular tooling changes to evade detection.

APT Group	Aliases	Affiliation	Focus Areas	Notable Incidents	Common TTPs
APT1	Comment Crew	PLA Unit 61398	Manufacturing, Energy, Critical Infrastructure	2013 Mandiant report exposure	Spear-phishing, custom malware, persistent access
APT3	Buckeye, Gothic Panda	Ministry of State Security	Aerospace, Defense, Energy	Use of DoublePulsar before public leak	Exploitation of vulnerabilities, credential theft
APT10	Stone Panda	Ministry of State Security	Managed Service Providers, Supply Chain	Cloud Hopper campaign (2014–2017)	Supply chain compromise, credential harvesting
APT27	Emissary Panda	Ministry of State Security	Political, Defense, Embassies	Targeted foreign embassies	Web shells, living-off-the-land, targeted phishing
APT41	Double Dragon	MSS Contractors	Healthcare, Software Supply Chains	COVID-19 research targeting, supply chain attacks	Zero-day exploitation, dual-use crime & espionage

China