I-Shou International School Model United Nations I 2025

Forum: General Assembly 1

Issue: (202) Enhancing cybersecurity resilience by combating social engineering vulnerabilities

Student Officer: John Weng (AST)

Position: Deputy Chair

Introduction

Cybersecurity, as defined by Kaspersky, is "the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks." Since the rise of technology and global networks in the 1970s and 80s, technology has rapidly evolved—along with it, so have the threats. Over time, digital attackers have modified their *modus operandi* (method), giving rise to various threats; one particular area that has received much attention is social engineering, which refers to the "manipulation [of] techniques that exploit human error to gain private information, access, or valuables" (Kaspersky). As cybersecurity rapidly improves, cyber-criminals tend to implement more social engineering tactics into their attacks, making it one of the key aspects that demands more urgent global attention.

Social engineering vulnerabilities did not become particularly prominent until the early 2000s, as companies, governments, and individuals began to encounter more cyberattacks that exploited social engineering vulnerabilities. This trend reached a critical point during the COVID-19 pandemic, as cyber-criminals obtained access to critical business assets and sensitive organizational data. During this period, Advanced Persistent Threat groups (APTs) were utilized to steal sensitive data that targeted high-value institutions and global leaders. Key examples include Russia's APT28, China's APT41, and North Korea's Lazarus Group unleashed phishing attacks to steal COVID-19 research and disrupt global supply chains. Simultaneously, the Brno University Hospital in the Czech Republic suffered ransomware attacks, where cybercrime groups deployed Ransomware-as-a-Service tactics through spear-phishing.

In the light of these threats, many cyber defense mechanisms—such as robust incident response plans, regular data backups, and safeguards—have been implemented to enhance resilience. Today, cybersecurity has become an essential pillar in modern society. Not only does it mitigate the effects of cyberattacks, but it also maintains business continuity and protects unauthorized information.

Despite these advancements, humans remain the first line of defense and the most vulnerable to cyberattacks. According to Verizon's 2023 Data Breach Investigations report, 74% of all cyber breaches were caused by human fallacy, misinterpretation, and error. Likewise, 48% of large companies have endured 25 or more

social engineering attacks, resulting in financial damage of up to $100,000. As a result, these vulnerabilities can pose significant risks to governments, private sectors, and people; this leads to mutual mistrust, financial losses, and the shutdown of business operations. With the increase of eminence and complexity, it becomes crucial to strengthen cybersecurity not only through the means of technology but also through social engineering.

It is undeniable that cybersecurity has been evolving rapidly. As it improved, so did the threats and prominence. Across the world, many cyber-criminals have exploited human behavior through social engineering tactics. To address this issue, people have implemented cyber defense mechanisms for the protection of unauthorized information and to maintain business continuity; however, human behavior and actions remain the weakest link because of how easily manipulated it is. Effectively solving this issue will require a combination of methods, from integrating weekly educational programs to teach people about the different forms of social engineering, to utilizing AI-detection systems to examine suspicious emails, documents, and links—all of which will depend on global cooperation, urgency, and awareness.

Definition of Key Terms

Cybersecurity resilience

The definition of "cybersecurity resilience", as stated by IBM (International Business Machines Corporation), means "an organization's ability to identify, respond, and recover swiftly from a cybersecurity incident." Enhancing cybersecurity resilience is critical to maintain a business or organization's business continuity, information security, and flow of operations. The commonly known tactics of cyberattacks include software code errors, insufficient security functions, and poor design. However, in this case, we discuss the social engineering aspect of cybersecurity.

Social engineering

Social engineering (in the context of cybersecurity) is when cyber-criminals take control of human behavior or emotions to trick the person into acting for them. Several factors, including a lack of digital literacy, natural human error, and the ease with which social engineering can be performed, collectively contribute to social engineering vulnerabilities. However, the main reason surrounding this sector is the vulnerability of people to human manipulation tactics, which allows unauthorized access to private information.

Advanced Persistent Threats (APTs)

Advanced Persistent Threat (APT) groups, also commonly referred to as APTs, are well-planned and sophisticated cyberattacks—targeting social engineering vulnerabilities (about 70-90%)[1]—that are orchestrated by highly experienced cyber-criminals to infiltrate specific networks with the primary goal of stealing significant data over an extended period. The term 'advanced persistent threat' originated in the U.S. Department of Defense at the start of the 21st century to describe persistent cyberespionage attacks from China. Their main targets are usually high-end, value-driven organizations. Tactics can range from spear-phishing strategies (which is phishing that is well-researched and very personalized) to backdoor schemes, which allow them to gain easy access to the organization's network and entire software.

Phishing

Phishing is a common form of cyberattack utilized by cyber-criminals in which one or multiple targets are contacted through email, text messages, or through telephone calls (mostly through email). These cyber-criminals often pose as executives to appear legitimate, which often easily acquires the individual's attention, and then they typically exploit human emotions (fear, urgency, curiosity) to gain their trust. This leads to long-term consequences, such as financial loss and identity theft.

Digital literacy

Digital literacy is the safe and smart use of a wide range of digital technologies utilized for communication, information, and problem-solving in all aspects of life. The UN addresses the evolving topic of digital literacy as a "regionally defined and culturally amplified topic." There have been multiple meetings pressuring the UN to take a proactive stance with the intent of implementing collaborative solutions, one of them being educating rural and less-developed member-states about digital literacy. This can allow people to understand and manage the information that they receive; in this context, determine if something is possibly trying to cyberattack them or not.

Institutional awareness

Institutional awareness is the understanding of all formal and informal structures of an organization; however, in this case, it can mean comprehending what weaknesses cyber-criminals may exploit in the system. Through the aspect of social engineering vulnerabilities, institutional awareness allows people to have a greater understanding of best practices utilized by cybercriminals and implement a sense of accountability for protecting sensitive data, which can help reduce the amount of social engineering cyberattacks.

Data breach

[1]Akerr. "Red Team Exercises against Social Engineering Attacks." *Outpost24*, 9 May 2025, outpost24.com/blog/red-teaming-and-social-engineering/.

A data breach, according to the UNDRR (United Nations Office for Disaster Risk Reduction), is "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored, or otherwise processed." It is also known as a cyber breach. Data breaches are extremely costly and business-threatening, with experts calculating damages of up to $5 trillion by 2024, primarily caused by malicious attacks and human errors. Keep in mind that not all cyberattacks are data breaches.

Background Information

The earliest origins of social engineering

Social engineering, a concept that has been around for millennia, can be traced back to 1184 BC, when the Greek soldiers devised a crafty plan to defeat the Trojans. The plan? They constructed a giant wooden horse and hid some of their army in it. The Trojans accepted the horse and allowed it to trot into the camp, not knowing it was a social engineering trap. After the sun set and the Trojans went to bed, the soldiers inside the horse snuck out and unlocked all gates leading into the city of Troy—sneaking in the rest of the Greek army. As a result, they used the element of surprise to obliterate the city of Troy, formally ending the war. This is a perfect example of early social engineering because it was deliberately planned to give the Trojan army false senses of comfort, trust, and safety.

Figure 1: A picture portraying the legendary Trojan horse being brought into Troy.

As time went on, social engineering could also be seen being utilized in warfare. One infamous example of this is the 1943-1944 Operation Fortitude during World War II, which highlighted many historical social

engineering tactics planned by the United States of America, the United Kingdom, France, and many others. Some of which include creating imaginary armies, deceptively realistic military vehicles and airfields, and hiring double agents and actors to feed the Germans false information. Of all these, the most effective tactic was the double agent tactic, with the Germans believing most of the double agents' statements. This was coincidentally also an act of social engineering. At last, they were misled about the location of the D-Day landings, which caught the German army off guard, leading to the fall of Nazi Germany.

Rise of technology and social engineering tactics

As technology evolved during the early 21st century, so did the attacks regarding social engineering. With cyber-criminals, hackers, and fugitives becoming increasingly prominent, the world was thrown into a period of "cyberattack-chaos." One of these attacks, known as Advanced Persistent Threats (APTs), which utilize sophisticated threats from various hackers, has slowly begun to emerge in daily life. The very first APT attack was called 'Titan Rain', which originated from China, and was a series of precise and coordinated attacks that were targeted towards U.S. government networks from 2003-2006 and involved a lot more technological applications rather than social engineering tactics. Managing to steal unauthorized sensitive data regarding the U.S. military, aerospace, and defense blueprints, Titan Rain constituted an extremely successful data breach. It was later revealed that the Chinese state-sponsored intelligence agencies utilized rootkits—malicious software that hid in the system, allowing for direct remote access.

One of the first APT attacks to exploit social engineering vulnerabilities was Operation Aurora—a series of precise, coordinated attacks believed to have been carried out by PLA Unit 61398 [2], possibly with assistance from Sneaky Panda and connections to Winnti Umbrella[3]. This attack targeted Google, Adobe, and dozens of other U.S. companies through many carefully conducted phishing campaigns, most of which included spear-phishing. From crafting forged emails that were tailored toward specific individuals to sending compromised, malicious websites, Operation Aurora employed various spear-phishing techniques, deliberately linking infected systems to command-and-control servers to gain unauthorized access to proprietary information and trade secrets. While the campaign successfully infiltrated multiple U.S. companies, it also risked jeopardizing China's access to the U.S. market. The incident is widely regarded as a milestone in recent cybersecurity history, demonstrating how easily cyber operations can be used as tools for industrial espionage.

Another very well-known and present APT attack also utilizing social engineering tactics was the 2016 DNC Email link, where the US Democratic National Committee received numerous phishing emails and malicious software from the Russian APT groups Cozy Bear (APT29) and Fancy Bear (APT28); however, these two APT groups worked separately. After vigorous searching, investigators found source code that was referenced back to previous

[2] PLA Unit 61398 is an APT originating from China
[3] Sneaky Panda and Winnti Umbrella are also APTs linked to China

APT groups in the DNC computers, which were coincidentally Cozy and Fancy Bear (nicknamed by security experts based on familiarity). Fancy Bear played the part of setting up tailored phishing websites that were extremely indistinguishable from the real ones to gain long-term espionage. At the same time, Cozy Bear employed backdoor spear-phishing methods to infiltrate the DNC's network by targeting specific hosts to influence the election in favor of their preferred candidate, President Donald Trump. This event was direct evidence of the Russian government's military intelligence agencies and the FSB trying to disrupt U.S. politics.

Overall, all three attacks had devastating consequences for the U.S.; however, there is one immensely distinct aspect that separates the two: the complexity of the attacks. While Titan Rain was an extremely successful data breach, gaining access to the U.S. Department of Defense, Department of Energy, and many others, it required many skills that present-day people do not possess. It required adequate understanding of wired and wireless systems, firewalls, and file systems, strong coding skills—all of which are extremely complex and take many years to perfect. Exploiting social engineering tactics, such as Operation Aurora and the 2016 DNC Email link incidents, takes less skill, is much easier to manipulate, and can pass various cybersecurity defenses through these tactics.

Present-day APT groups

Nowadays, APT groups are everywhere; however, they remain undetected to protect their identity. These APT attacks still target a diversity of industries across nations, with the most targeted industries being information technology, finance, and manufacturing. According to Cyfirma, which specializes in decoding threats and recording APT attacks on industries, states, "the overall number of APT attacks has increased by 15%," suggesting that the APT landscape is still shifting and rapidly developing.

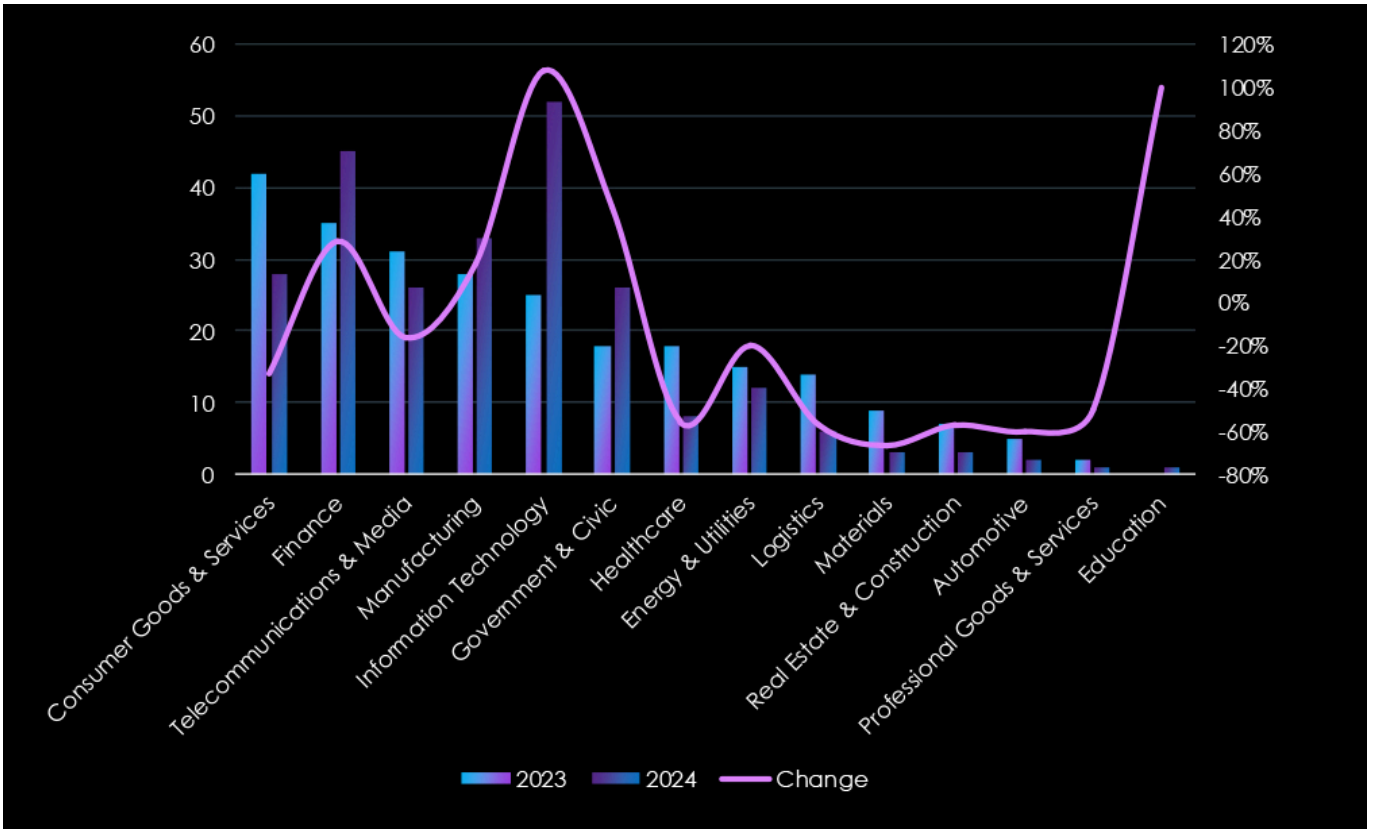

Figure 2: A bar chart displaying which sectors were affected the most by APT attacks.

They are all across the globe—in Europe, Asia, the Middle East, et cetera. There is no doubt that APT groups have taken the world by storm, with some of the world's largest APT providers including Iran, Russia, China, and North Korea. With further investigation, it is revealed to the public that most of these APT attacks are either state-sponsored, supported by governments, or operating via private institutions. However, it has become clear that most of these APTs are originating from China, with almost half of the APT attacks traced back to China through past data records. In Figure 2, one may come to think that the origination of these APT groups is spread evenly; however, in Figure 3, it is evident that China's percentage of originating APT groups dominates the bar chart. In conclusion, APT groups remain a prominent issue today, and their devastating attacks require more attention than they are given.

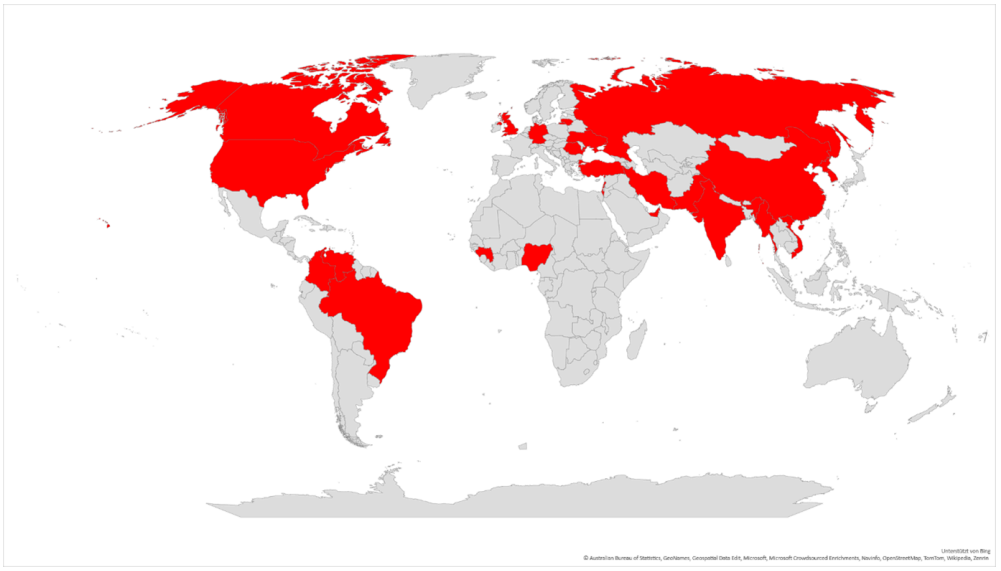

Figure 3: A map displaying the countries from which the APT groups originated.

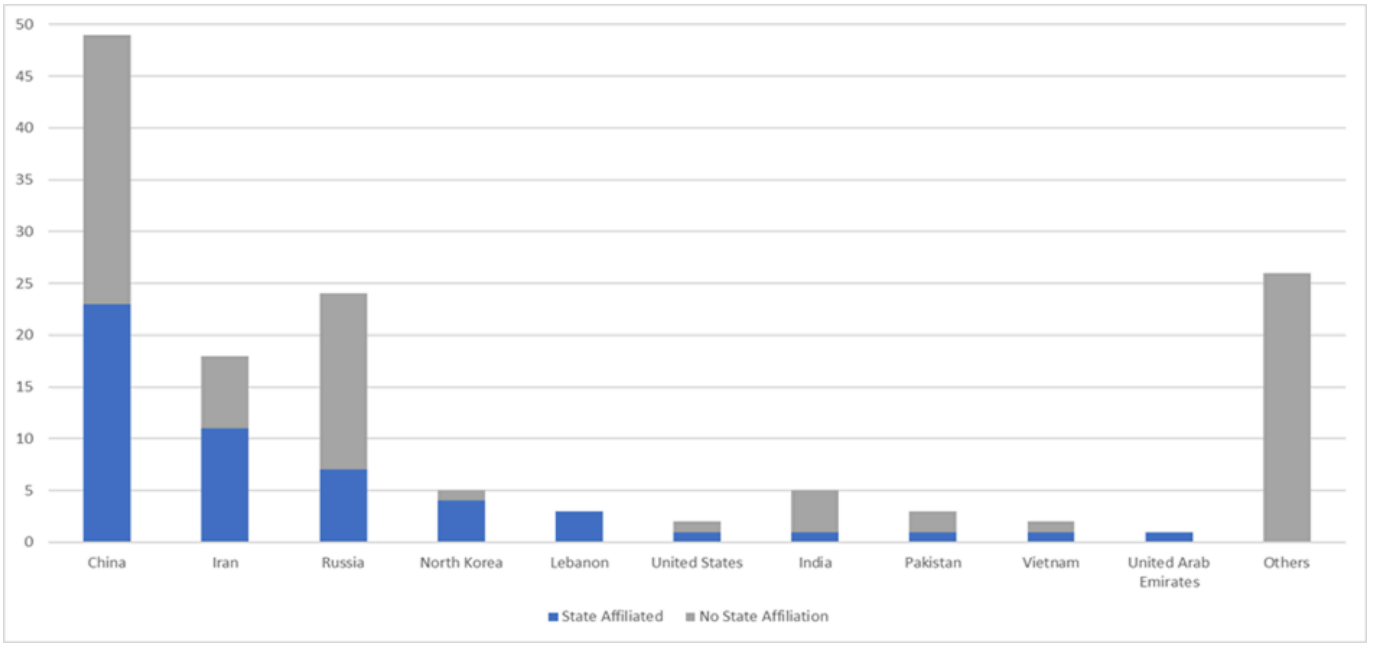

Figure 4: A bar chart displaying the leading countries ranked by origin of APT.

Key Issues

Lack of digital literacy understanding and training

Being vulnerable to social engineering attacks is a serious security flaw that exposes individuals, businesses, and even nations to severe consequences. As AI continues to develop and evolve, it becomes

increasingly difficult for people to distinguish between legitimate and illegitimate forms of social engineering, which is the reason why having a clear understanding of social engineering attacks is emphasized.

According to the latest industry benchmarking report, 34.3% of employees fail phishing tests. At the same time, a recent survey of 2,000 UK workers found that 56% couldn't distinguish between AI-generated scam emails and legitimate ones. These findings highlight a critical issue: without adequate understanding and training, individuals can unintentionally expose sensitive information—ranging from financial data to political strategies—to advanced persistent threats (APTs) and cybercriminals.

A prime example is the 2016 DNC cyberattack. When Hillary Clinton's campaign chair, John Podesta, received a phishing email, a staffer mistakenly marked it as legitimate. This led Podesta to unknowingly enter his real credentials, giving hackers access to his private inbox. As a result, confidential communications, donor information, and internal political discussions were leaked. This breach stemmed directly from a lack of cybersecurity awareness and training. Many employees place too much trust in their organization's IT systems, assuming they're fully protected from threats. However, as this case shows, human error remains the most exploitable vulnerability, and training is the only effective defense.

Lack of international awareness and recognition

There is a huge difference in international awareness between cybersecurity and other more valued topics. For example, the UN has over four thousand articles, resolutions, and campaigns dedicated to the promotion and protection of human rights; however, it has less than fifty pages committed to cybercrime, and certainly not enough actions and frameworks taken to prevent cybercrime, with most of the articles covering cybercrime have expressed their views on the evolving and growing threats in all forms. This topic is also rarely discussed in UN summits and deserves more recognition than it currently has, given the devastating consequences through the provided past and present examples.

Every so often, there would be a call to action for the purpose of facilitating improved and managed communications for people on the internet, urging the need for international cooperation between nations, and pushing for the undivided international cooperation between nations. The main problem was that it was not very prominent and was an issue that was talked about daily in colloquial and formal talks. As technology improves and social engineering tactics become ever-increasingly prominent, it is hoped that the landscape of cybercrime regarding social engineering becomes more alarming and threatening globally. Subsequently, it may potentially raise the attention of global leaders, company executives, and employees, and the eyes of the people.

Major Parties Involved and Their Positions

China

China has proved itself to be a highly involved country regarding this issue. From China's APT40 and Mustang Panda, which is estimated to account for 46% of all APT activity, to China-supported APT41, showing a substantial increase in activity in the first quarter of 2025, it is evident that China is one of the leading APT providers today through the course of social engineering attacks. For years, the Chinese government has been accused of financially helping out these APT groups. Many countries (Singapore, the United States, even ROC, and others) are pretty confident that the Chinese government has supported them in different ways. Although there has been concrete evidence from various incidents that directly relates to the MSS[4], JSSD[5], and many other Chinese government intelligence agencies, the Chinese Embassy in Washington has denied all accusations and has stated that China opposes "cyber threats in all forms." Despite that, China has implemented various cybersecurity laws to fight telecom and internet fraud and establish a safe, multilateral, and transparent "cyber sovereignty" (as stated by DigiChina). Not only that, but it has also emphasized the need for collaboration between nations to combat the criminal usage of information and communications technology. As a result, China has been an active UN member in fighting for the responsibilities and international norms that states should keep in mind about the growing threat of cybersecurity; however, it should be a key actor to watch, given the unpredictability of its cyber strategy and the PLA's[6] continuously growing interest in 'cognitive warfare'.

United States

The United States has had an abundance of experience dealing with cyber threats, particularly from state-sponsored Advanced Persistent Threat (APT) groups originating from China and Russia. As the most targeted country globally, the U.S. continues to face significant cybersecurity challenges. According to Trellix, a global cybersecurity research firm, there was a 136% increase in cyber threat detections targeting the U.S. in Q1 2025, compared to Q4 2024. These attacks have compromised sensitive networks, email servers, and national security infrastructure.

The U.S. government has repeatedly expressed concerns over the growing sophistication of China-linked cyber operations, warning that these campaigns often target critical infrastructure, federal agencies, and the telecommunications sector. In past administrations, efforts were made to bolster U.S. cyber defenses through the Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Cyber Command. Furthermore, the U.S. Department of Justice has imposed sanctions on actors targeting U.S. government entities and companies, showing its concern about the evolving world of cybersecurity.

[4] The MSS is the Ministry of State Security
[5] The JSSD is the Jiangsu State Security Department
[6] PLA is China's armed forces

However, during the Trump administration, there was a notable rollback in certain cybersecurity initiatives, including a reduction in CISA's resources and a pause in cyber operations against Russia. These decisions drew criticism from cybersecurity experts, who warned that such moves could weaken the nation's resilience against foreign cyber threats. This has led to ongoing debates about the long-term dependability and leadership of the U.S. in cybersecurity governance.

Russian Federation

The Russian Federation is frequently assessed by cybersecurity experts as the second-largest state sponsor of Advanced Persistent Threat (APT) operations in the world, following closely behind China. Multiple Russian state-linked APT groups—such as APT28 (Fancy Bear), APT29 (Cozy Bear), and APT44 (Sandworm)—have targeted foreign governments, institutions, and infrastructure, primarily through spear-phishing campaigns. A notable example occurred during the early stages of the Ukraine-Russia War, when the cyber-espionage group Gamaredon was described by the EU's CERT-EU as the "most prolific actor" at the time. Using aggressive phishing emails embedded with malware-laced documents, Gamaredon not only disrupted Ukrainian targets but also disseminated Russian propaganda.

Further investigations have revealed that Russian intelligence agencies, particularly the FSB, GRU, and SVR, often work closely with cybercriminal organizations when their goals align. In many cases, these relationships are informal, with intelligence operatives embedding within or overseeing the activities of APT groups. Leaks involving actors like Conti, TrickBot, and BlackBasta have exposed longstanding and coordinated links between these criminal networks and Russian intelligence agencies, which many experts may interpret as strong evidence of the involvement of Russian government officials and cybercriminal networks. Despite this, Russia has been a prominent actor in the GA1 committee, frequently submitting views to the UN Secretary-General about cyberspace, and has called for new global rules to regulate cyber activity while maintaining a sovereign stance.

However, Russia denies all attributions to Russian-originated APTs and has consistently brought up the technological difficulties and anonymity challenges that may result in tracing back to the original perpetrators. It states that there has been no concrete evidence to support the conjectures addressing the connection between the Russian government and APTs, and that they are so-called "political attributions" that make the committee extremely "unconstructive and misleading".

Türkiye

Türkiye is one of the major parties that has encountered and dealt with multiple social engineering attacks. Research has stated that over 80 companies in Türkiye are being targeted through spear-phishing emails, and about $5.2 billion worth of bitcoin has been stolen from Türkiye. To counter numerous APT threats, Türkiye

has enacted a new cybersecurity framework law (No. 7545) to recognize and emphasize cybersecurity, with the intent of evaluating principles and actions that would best protect critical infrastructure and create a safe cyberspace. This law introduces compliance obligations towards public and private sectors, typically ones that focus on infrastructure, and is coordinated with already-enacted laws, such as the KVKK, which states to protect unauthorized data (to build an established framework). Lastly, Türkiye has actively participated in NATO, publishing documented reports that underscore best practices utilized in their country, which have helped other nations with their cybersecurity governance and improved awareness in the cybersecurity foundation.

Iran

Iran, with cybersecurity experts classifying it as the third-largest APT producer and one of the more involved parties in this issue, usually utilizes state-sponsored APT groups that align with their interests, such as APT35. Operated through Iran's intelligence agencies, these APTs engage in cyberespionage campaigns that target the Middle East and Europe, the U.S. being more prominently targeted in these attacks. Despite numerous sanctions placed by the U.S. Treasury on Iranian APTs, companies, and individuals involved in malicious cyber attacks, Iran's state-sponsored APTs continue to expand their cyber attack interests, protect their operational security, and adapt to continuously evolving cyber defenses. However, there is no actual evidence stating Iran's official stance, or as a matter of fact, they have made zero efforts to solve the issue.

North Korea

North Korea has had multiple state-sponsored APTs that have targeted nations in various ways. Whether it's through posing as executives or inviting employees to fake Zoom meetings, North Korea has done it all. Due to how easily manipulable people are, the malicious packages given through emails have impressively amassed over a total of 17,000 downloads—their fake job and employee impersonation attacks are infamous, likely because these attacks are carefully researched and target software supply chains (which include npm packages[7]). Furthermore, North Korea has stolen over $700 million in cryptocurrency through cyberattacks and sent more than 120,000 phishing emails to over 18,000 individuals—certainly a country to look out for. However, just like Iran, North Korea has made no efforts, public announcements, or anything to solve the issue.

Republic of China

Being the world's most geopolitically significant semiconductor industry, the Republic of China (also known as Taiwan) has dealt with innumerable APTs and cyberattacks, most of them originating from China. According to Reuters, cyberattacks on the Republic of China "doubled in 2024 from the previous year to an average of 2.4 million attacks a day," as stated by the Republic of China's National Security Bureau. These APTs are

[7] Npm packages - used to find and manage code packages (in terms of this issue, it's used for harm)

primarily targeting the Republic of China's organizations and businesses that focus on semiconductor making and military drills around the island, with the intent of not only intensifying intimidation but also leveraging their power in the global semiconductor supply competition. In response, the Republic of China has implemented 17 security measures to combat the ever-mounting and evolving threats encircling the industry, many of them intended to prevent social engineering tactics. It was based upon President Lai's dedication to safeguard and protect the Republic of China's sovereignty.

Timeline of Events

Date	Description of event
1184 BC	The Trojan War is considered one of the earliest forms of social engineering. The horse was deliberately planned to be offered to the Trojans to give them a false sense of comfort, trust, and safety.
March 4, 1943-June 6, 1944	Operation Fortitude, which was commissioned by the U.S., the UK, France, and Canada, is another extremely significant and effective social engineering deception that was utilized to mislead the Germans about the invasion of Europe.
November 1, 2003	One of the first APT attacks, Titan Rain, was a successful breach that targeted U.S. government networks and involved more technological applications than social engineering tactics. They utilized rootkits for remote access and unauthorized information-gaining to cause chaos in U.S. politics
March 26, 1999	The Melissa Virus utilized tempting messages to execute its plan. It wreaked havoc, disrupted the internet, and shut down over 300 government corporations and agencies across the planet,
May 4, 2000	The 'ILOVEYOU' virus, which originated in the Philippines and infected millions of computers worldwide, was disguised as a 'love letter' that tricked people into opening a malicious attachment. It resulted in a financial loss of $3 billion to $15 billion.
June 12, 2009	Operation Aurora was the first APT attack ever to exploit social engineering vulnerabilities. It targeted U.S. companies, such as Google and Adobe, through sophisticated spear-phishing tactics.

December 27, 2019	The GA3 committee adopted Resolution 74/247 on "Countering the use of information and communications technologies for criminal purposes," initiating a process toward a global treaty on cybercrime, focusing on sovereignty and equal participation.
December 24, 2024	The UN Cybercrime Convention was the first encompassing treaty that was established to focus on all aspects of cybercrime. It has already been adopted and will soon be open for ratification on October 25, 2025.
June 26, 2025	A Nigerian man was placed under charges for being involved in a million-dollar business email compromise and email fraud scam. The attack targeted companies in eight U.S. states, with people being tricked into transferring money to fraudulent bank accounts.
July 21, 2025	The North Korea-linked threat actor known as Kimsuky has exploited the social engineering factor by impersonating South Korean executives. They then instructed employees to run and paste the malicious code sent through phishing emails.

Relevant UN Resolutions, Treaties, and Events

- Resolution 74/247, 27 December 2019 (**A/RES/74/247**)

  Resolution 74/247 was a resolution that focused on countering informational and communicational technologies for criminals (which social engineering was a part of). It listed previous resolutions and various alarming facts about cybercrime to gain the attention of nations worldwide. To solve this issue, the resolution mainly stressed national and international cooperation by establishing a permanent ad hoc committee to include all representatives of nations, organizations, and experts.

- GA1 Proposes New Action for the Struggle Against Cybersecurity, 18 October 2021 (**GA/DIS/3673**)

  This GA1 session is specifically picked due to the fact that it tailors toward discussions, draft resolutions, and collaborations about the dangers and solutions of cybersecurity in different forms—a topic rarely talked about in the UN. Not only did it talk about mitigating cybersecurity attacks, but it also discussed the disarmament of nuclear warfare. The session proved to be highly successful and productive, with representatives from various countries voicing their concerns about the escalating waters of cybersecurity threats and highlighting best practices to address them.

- Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, 12 September 2011 (**GA A/66/359**)

  This letter's central direction focused on the rights and responsibilities of neighboring states in the information landscape, further encouraged each state's responsible and productive behaviors, and ensured that all forms of technology were utilized to benefit only social and economic development and preserve international security and stability. These methods may seem very collaborative and internationally-focused; however, the letter focused on a more sovereign scope, with the code of conduct pledging all nations that signed the treaty to uphold international norms regarding sovereign integrity, territorial integrity, and political independence, which degrades the overall purpose of the UN.

- UN Secretary-General Warns of Cyber Mercenaries Amid Spike in Weaponizing Digital Tools, 20 June 2024

  During a Security Council high-level discussion, present-day Secretary-General António Guterres highlighted the evolving power of digital technologies by making several remarks throughout the course of the debate. He addressed the benefits of ever-growing technology, such as how it brings people together and interact with government services online. However, he underscored the easy and quick connectivity of the internet that made nations vulnerable to cybercrime.

- United Nations Convention Against Cybercrime, 24 December 2024 (**A/RES/79/243**)

  The UN Cybercrime Convention, which was the first treaty that was initiated by resolution 74/247, was just recently established to combat crimes regarding ICTs (Information and Communication Technology). It was the first comprehensive treaty that focused on all aspects of cybercrime, and aimed to not only strengthen international cooperation regarding this issue (since it had less attention compared to other issues), but also promote technical assistance and capacity-building systems, and strengthen measures utilized to combat cybercrime. This treaty will be in force after a planned signing ceremony on October 25, 2025, in Hanoi, Vietnam.

Evaluation of Previous Attempts to Resolve the Issue

The 2011 Letter submitted by China, the Russian Federation, Uzbekistan, and Tajikistan addressed to the United Nations Secretary-General

The 2011 letter (proposed by China, Russia, Uzbekistan, and Tajikistan) underscored that states were the key actors in cyberspace and highlighted each state's basic rights and responsibilities to combat cybercrime. While they did follow the Charter of the United Nations[8] and proposed various significant solutions towards the issue, it had a large focus on maintaining each state's sovereignty, state control, and non-interference in cyberspace. This, although it was a political declaration, sought to eventually suggest essential principles, which would later be bound into an international agreement that directed the behavior of states in cyberspace. As a result, this proposal was unable to obtain the approval and widespread support among all UN member states, due to its excessive focus on sovereignty for states. Key states such as the US and UK, which largely advocate for freedom of expression and a more open cyberspace, opposed it.

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was established in 2001 as a framework to enable member states to share experiences and foster cooperation on best practices, particularly in emergencies. According to the Council of Europe, "Any country may make use of the Budapest Convention as a guideline, checklist or model law," which can help states realize their strengths and weaknesses when establishing their laws through collaboration.

The framework's overall focus was to provide a "free internet" where information can be freely shared and accessed. Recognizing that technology is constantly evolving, which leaves states, organizations, and businesses vulnerable to cybercrime, the Budapest Convention on Cybercrime collects data when necessary while also adhering to traditional norms regarding human rights. Furthermore, it also utilizes capacity-building projects to support other member states in the prosecution of cybercrime in all forms. This framework has already been ratified by over 70 countries; however, it has not yet been ratified by key countries, such as Russia and China, which argue that the convention is too biased and non-universal. It leaves the global landscape of cybersecurity divided, questioning the overall cooperation.

Possible Solutions

Having a clear and undisputable definition of social engineering

The term "social engineering" can be dangerously vague. Generally, the universally accepted definition of social engineering is "[the] exploiting [of] human behavior with the intent of gaining sensitive or unauthorized information." However, some may interpret social engineering as "manipulating public opinion through media or cultural influence on a broad scale." This ambivalence makes enacting precise laws, resolutions, and treaties a

[8] The UN Charter highlighted the sovereign equality of each state, solidified the crucial principles of international relations, and prohibited the use of force in international relations.

complicated and frustrating process, since a poorly defined term can have unexpected consequences, sparking a global crisis and increasing international tensions. Furthermore, these types of complications and problems mainly happen when a member-state gains adequate leverage and power to push forward its interpretations or agenda; a clear definition of social engineering allows for a clear purpose and prevents political and sovereign domination when drafting frameworks and resolutions. Ultimately, clarifying the definition of social engineering allows for government officials, organizations, and buildings to implement productive solutions while not having to worry about vague wording that can be exploited to bypass traditional international norms.

Enacting more international frameworks that focus on social engineering vulnerabilities

Most frameworks, resolutions, and discussions primarily focus on cybersecurity; however, they often do not explicitly emphasize the aspect of social engineering and its vulnerabilities, or sometimes overlook it at significant times. Given previous events and evidence, social engineering is a critical component that should not be ignored (as evidenced by previous events); if not addressed, states tend to miss the root cause of these attacks. This aspect has already been emphasized by the 2024 International Criminal Police Organization (INTERPOL)'s awareness campaign, which promotes cybersecurity awareness, informed decision-making, and vigilance in cyberspace. However, the UN still barely recognizes the importance of social engineering attacks and lists them as a "secondary concern" in the broader cyberspace world; this is due to a lack of understanding of their severity and international recognition.

Enacting international frameworks that specifically focus on social engineering vulnerabilities can facilitate neutral information sharing, as member states are highly divided on this issue. The framework should focus on universally agreed-upon topics, such as capacity-building measures, institutional awareness, or digital literacy to combat social engineering attacks. Not only that, it should avoid politically sensitive or controversial topics that may prevent the house from reaching a consensus. One key example of this was Resolution 74/247. While it was not favored by all member states (because of their stance), they agreed on some key ideas, with the most common agreed-upon aspects being fostering best practices regarding this issue, since social engineering is universally recognized as a criminal threat to society and practices that do not go against traditional norms are most likely to be approved by all sides of the house. However, this solution may be more challenging to implement due to the obstinate focus of various countries on sovereignty.

Bibliography

"What Is Social Engineering: Attack Techniques & Prevention Methods: Imperva." *Learning Center*, Imperva, 20 Dec. 2023, www.imperva.com/learn/application-security/social-engineering-attack/.

"About the Convention - Cybercrime - Www.Coe.Int." *Council of Europe*, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 31 July 2025.

"About the Convention - Cybercrime - Www.Coe.Int." *Council of Europe*, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 31 July 2025.

Bagwe, Mihir. "North Korean Hackers Targeted Nearly 18,000 in Phishing Campaign during Martial Law Turmoil." *The Cyber Express*, 16 Apr. 2025, thecyberexpress.com/north-korean-hackers-martial-law-phishing/.

Baker, Kurt. "What Is an Advanced Persistent Threat (APT)?" *CrowdStrike*, 2025, www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/.

A bar chart displaying the leading countries ranked by origin of APT. 28 Aug. 2023. *Origin & Evolution: An In-Depth Exploration of Advanced Persistent Threat (APT) Groups*, https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/. Accessed 30 July 2025.

A bar chart displaying which sectors were affected the most by APT attacks. 13 Jan. 2025. *CYFIRMA ANNUAL INDUSTRIES REPORT : PART 1*, https://www.cyfirma.com/research/cyfirma-annual-industries-report-part-1/ . Accessed 30 July 2025.

"Basic Facts about the Global Cybercrime Treaty." *United Nations*, United Nations, www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty. Accessed 31 July 2025.

Bowcut, Steven. "How to Become an Ethical Hacker: A Blueprint." *Cybersecurity Guide*, 15 Apr. 2025, cybersecurityguide.org/resources/ethical-hacker/.

"Brno University Hospital Ransomware Attack (2020)." *International Cyber Law: Interactive Toolkit*, International cyber law: interactive toolkit, 3 June 2021, cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020).

Brown, Deborah. "Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks." *Human Rights Watch*, 28 Apr. 2022, www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks.

Chen, Ketty W. "President Lai Ching-Te's 17 National Security Measures: A Timely Proposal to Bolster the Safety of Taiwan." 遠景基金會, 22 Apr. 2025, www.pf.org.tw/tw/pfch/13-11279.html.

"Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years." *Office of Public Affairs | Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years | United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.

Clementi, Andreas. "Origin & Evolution: An in-Depth Exploration of Advanced Persistent Threat (APT) Groups." *AV*, 19 Mar. 2024, www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/.

"Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora." *Council on Foreign Relations*, Council on Foreign Relations, Jan. 2010, www.cfr.org/cyber-operations/operation-aurora.

Creemers, Rogier, et al. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *DigiChina*, 16 Aug. 2022, digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

"Cyber Defense - the Complete Guide." *Tenable®*, www.tenable.com/source/cyber-defense. Accessed 30 July 2025.

Doyle, Kirsten. "Understanding Social Engineering Tactics: 8 Attacks to Watch out For." *Social Engineering: Definition & 5 Attack Types*, 2024, www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for.

Dyck, Brent Douglas. "Operation Fortitude: The Great Deception." *Warfare History Network*, 18 July 2022, warfarehistorynetwork.com/article/operation-fortitude-the-great-deception.

Fadilpašić, Sead. "North Korean Hackers Release Malware-Ridden Packages into NPM Registry." *TechRadar*, TechRadar, 15 July 2025, www.techradar.com/pro/security/north-korean-hackers-release-malware-ridden-packages-into-npm-registry.

Flashpoint Intel Team. "Evolving Tactics: How Russian Apt Groups Are Shaping Cyber Threats in 2024." *Flashpoint*, 8 July 2025, flashpoint.io/blog/russian-apt-groups-cyber-threats/.

Fokker, John. "The Cyberthreat Report: April 2025." *Trellix*, Apr. 2025, www.trellix.com/advanced-research-center/threat-reports/april-2025/.

Greenberg, Andy. "US Charges 12 Alleged Spies in China's Freewheeling Hacker-for-Hire Ecosystem." *Wired*, Conde Nast, 5 Mar. 2025, www.wired.com/story/us-charges-12-alleged-spies-in-chinas-freewheeling-hacker-for-hire-ecosystem/.

"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations*, United Nations, 22 July 2015, docs.un.org/en/a/70/174.

Group, negg. "Cyber Trump: Why Slashing U.S. Digital Defenses Could Backfire ." *Negg Blog*, 17 Apr. 2025, negg.blog/en/cyber-trump-why-slashing-u-s-digital-defenses-could-backfire/.

Halisdemir, Erme. "National Cyber Security Organisation: Turkey." *CCDCOE*, ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/. Accessed 31 July 2025.

"The History of Social Engineering." *Mitnick Security Consulting*, www.mitnicksecurity.com/the-history-of-social-engineering. Accessed 30 July 2025.

History.com Editors. *A picture portraying the legendary Trojan horse being brought into Troy.* 18 Dec. 2009. *Trojan War*, https://www.history.com/articles/trojan-war. Accessed 30 July 2025.

"Interpol Campaign Warns against Cyber and Financial Crimes." *INTERPOL*, 3 Dec. 2024, www.interpol.int/en/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes.

Kaspersky. "What Is Cybersecurity?" *Kaspersky*, 30 July 2025, www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

KnowBe4. "What Is Phishing?" *Phishing*, www.phishing.org/what-is-phishing. Accessed 30 July 2025.

Korzak, Elaine. "Russia's Cyber Policy Efforts in the United Nations." *CCDOE*, 2021, ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf.

Kosinski, Matthew. "What Is a Data Breach?" *IBM*, 22 July 2025, www.ibm.com/think/topics/data-breach.

Lakshmanan, Ravie. "Bluenoroff Deepfake Zoom Scam Hits Crypto Employee with Macos Backdoor Malware." *The Hacker News*, 7 July 2025, thehackernews.com/2025/06/bluenoroff-deepfake-zoom-scam-hits.html.

Lakshmanan, Ravie. "Donot Apt Expands Operations, Targets European Foreign Ministries with LoptikMod Malware." *The Hacker News*, 10 July 2025, thehackernews.com/2025/07/donot-apt-expands-operations-targets.html.

Lakshmanan, Ravie. "Hackers Target over 70 Microsoft Exchange Servers to Steal Credentials via Keyloggers." *The Hacker News*, 24 June 2025, thehackernews.com/2025/06/hackers-target-65-microsoft-exchange.html.

Lakshmanan, Ravie. "Iranian APT35 Hackers Targeting Israeli Tech Experts with AI-Powered Phishing Attacks." *The Hacker News*, 26 June 2025, thehackernews.com/2025/06/iranian-apt35-hackers-targeting-israeli.html.

Lakshmanan, Ravie. "North Korea-Linked Supply Chain Attack Targets Developers with 35 Malicious NPM Packages." *The Hacker News*, 25 June 2025, thehackernews.com/2025/06/north-korea-linked-supply-chain-attack.html.

Lakshmanan, Ravie. "North Korean Hackers Exploit Powershell Trick to Hijack Devices in New Cyberattack." *The Hacker News*, 12 Feb. 2025, thehackernews.com/2025/02/north-korean-hackers-exploit-powershell.html?m=1.

Lakshmanan, Ravie. "U.S. Agencies Warn of Rising Iranian Cyber Attacks on Defense, OT Networks, and Critical Infrastructure." *The Hacker News*, 2 July 2025, thehackernews.com/2025/06/us-agencies-warn-of-rising-iranian.html.

Lee, Yimou. "Chinese Cyberattacks on Taiwan Government Averaged 2.4 Mln a Day in 2024, Report Says | Reuters." *Reuters*, 6 Jan. 2025, www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/.

Levi, Ran. "Malicious Life Podcast: Fancy Bear, Cozy Bear." *Cybersecurity Software*, www.cybereason.com/blog/malicious-life-podcast-fancy-bear-cozy-bear. Accessed 30 July 2025.

A map displaying the countries from which the APT groups originated. 23 Aug. 2023. *Origin & Evolution: An In-Depth Exploration of Advanced Persistent Threat (APT) Groups*, https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/. Accessed 30 July 2025.

Matthews, Tim. "Operation Aurora – 2010's Major Breach by Chinese Hackers." *Exabeam*, 21 May 2025, www.exabeam.com/blog/infosec-trends/operation-aurora-2010s-major-breach-by-chinese-hackers/.

Mendell, Ronald. "Advanced Persistent Threat." *Encyclopædia Britannica*, Encyclopædia Britannica, inc., www.britannica.com/topic/advanced-persistent-threat. Accessed 30 July 2025.

Ministry of Foreign Affairs, et al. "North Korea Using Social Engineering to Enable Hacking ..." *Joint Cybersecurity Advisory*, 1 June 2023, media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF.

Mishra, Vibhu. "UN Chief Warns of 'cyber Mercenaries' amid Spike in Weaponising Digital Tools | UN News." *United Nations*, United Nations, 20 June 2024, news.un.org/en/story/2024/06/1151266.

"Nigerian National Arrested in Multimillion-Dollar Email and Money Laundering Scam." *United States Attorney Office | Southern District of Texas*, 26 June 2025, www.justice.gov/usao-sdtx/pr/nigerian-national-arrested-multimillion-dollar-email-and-money-laundering-scam.

Okunytė, Paulina. "Half of Workers Still Can't Spot a Phishing Scam, Even When They Think They Can." *Cybernews*, 6 June 2025, cybernews.com/security/business-phishing-scams-detection/.

Plumb, Charlie. "Understanding the UN's New International Treaty to Fight Cybercrime." *United Nations University*, 30 July 2024, unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

"Resolution Adopted by the General Assembly on 24 December 2024." *United Nations*, United Nations, 31 Dec. 2024, docs.un.org/en/A/RES/79/243.

"Resolution Adopted by the General Assembly on 27 December 2019." *United Nations*, United Nations, 20 Jan. 2020, docs.un.org/en/A/Res/74/247.

Rutayisire, Alixia Clarisse. "The Proxy Warfare: Unmasking Russia's Externalized Cyber Capabilities." *QuoIntelligence*, 30 June 2025, quointelligence.eu/2025/06/proxy-warfare-russia-externalized-cyber-capabilities/.

Secretariat of the Cybercrime Convention Committee. "The Budapest Convention on Cybercrime: Benefits and Impact in Practice." *Council of Europe*, 13 July 2020, rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

Sjouwerman, Stu. "[Mastering Minds] China's Cognitive Warfare Ambitions Are Social Engineering at Scale." *KnowBe4 Security Awareness Training Blog*, KnowBe4, Inc., 26 May 2023, blog.knowbe4.com/mastering-minds-chinas-cognitive-warfare-ambitions-are-social-engineering-at-scale.

Tahir. "🕵️ Titan Rain: How Cybercriminals Hacked the United States Cyberspace." *Medium*, Medium, 23 Dec. 2024, medium.com/@tahirbalarabe2/%EF%B8%8F-titan-rain-how-cybercriminals-hacked-the-united-states-cyberspace-8add64ca512f.

Talihärm, Anna-Maria. "Towards Cyberpeace: Managing Cyberwar through International Cooperation." *United Nations*, United Nations, 12 Aug. 2013, www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

Technologies, Configr. "The Art of Deception: Social Engineering Tactics and How to Prevent Them." *Medium*, Medium, 28 July 2024, configr.medium.com/the-art-of-deception-social-engineering-tactics-and-how-to-prevent-them-54babf0840f6.

Toback, Michael. "Advanced Persistent Threat and Social Engineering Explained." *Endpoint Security*, 29 Oct. 2024, smallbizepp.com/apt-and-social-engineering/.

Traynor, Orlaith. "An Insider Look at Chinese Apt Threats." *CybelAngel*, 20 Jan. 2025, cybelangel.com/cyber-espionage-apts/.

"Turkey: Part One - Turkey Enacts Its First Cybersecurity Framework Law, a Pillar of National Security." *Dataguidance*, 4 May 2025, www.dataguidance.com/opinion/turkey-part-one-turkey-enacts-its-first.

Tzavara, Vasiliki, and Savvas Vassiliadis. "Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review - International Journal of Information Security." *SpringerLink*, 1 Feb. 2024, link.springer.com/article/10.1007/s10207-023-00811-x.

"UN Calls for Urgent Action to Enable Opportunities, Mitigate Risks for Information and Digital Technology." *United Nations*, United Nations, 12 Oct. 2023, www.un.org/en/desa/un-calls-urgent-action-enable-opportunities-mitigate-risks-information-and-digital.

"United Nations Convention against Cybercrime." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/cybercrime/convention/home.html. Accessed 30 July 2025.

"USA and South Korea Warn over North Korean Cyberattacks." *Digital Watch Observatory*, 7 June 2023, dig.watch/updates/usa-and-south-korea-warn-over-north-korean-cyberattacks.

Vicens, A.J., et al. "North Korean Cyber Spies Created U.S. Firms to Dupe Crypto Developers ." *Reuters*, 24 Apr. 2025, www.reuters.com/sustainability/boards-policy-regulation/north-korean-cyber-spies-created-us-firms-dupe-crypto-developers-2025-04-24/.

Wadhani, Sumeet. "What Is Social Engineering and Why Does It Work? - Spiceworks." *Spiceworks*, Oct. 2024, www.spiceworks.com/it-security/cyber-risk-management/articles/social-engineering-still-rampant/.

Walker, Summer, and Ian Tennant. “Control, Alt, or Delete? The UN Cybercrime Debate Enters a New Phase.” *Global Initiative*, Dec. 2021, globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf.

Walker, Summer, and Ian Tennant. “Control, Alt, or Delete? The UN Cybercrime Debate Enters a New Phase.” *Global Initiative*, Dec. 2021, globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf.

Wang, Zuoguang, et al. “Defining Social Engineering in Cybersecurity | IEEE Journals & Magazine | IEEE Xplore.” *IEEE Xplore*, IEEE, 2020, ieeexplore.ieee.org/abstract/document/9087851.

Wei, Changhao, and Taige Hu. “Legislation Summary: China’s New Law to Fight Telecom and Internet Fraud.” *NPC Observer*, 10 Oct. 2022, npcobserver.com/2022/09/07/legislation-summary-chinas-new-law-to-fight-telecom-and-internet-fraud/.

“What Is Social Engineering? - Definition, Types & More: Proofpoint Us.” *Proofpoint*, 14 July 2025, www.proofpoint.com/us/threat-reference/social-engineering.

Williams, Austin. “Defense Secretary Pete Hegseth Pauses US Cyberoperations against Russia.” *LiveNOW from FOX | Breaking News, Live Events*, LiveNOW from FOX, 4 Mar. 2025, www.livenowfox.com/news/hegseth-pauses-us-cyberoperations-russia.

“🇮🇷 APT35. Charming Kitten.” *Global Institute for National Capability*, Global Institute for National Capability, 18 Jan. 2025, www.ginc.org/apt35.

“Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General .” *United Nations*, United Nations, 14 Sept. 2011, docs.un.org/en/A/66/359.

KAYA, Dr. Mehmet Bedii. “Turkish Cyber Security Law No. 7545 Full Translation.” *Mbkaya*, mbkaya.com/hukuk/turkish-cyber-security-law-translation.pdf. Accessed 10 Aug. 2025.

“Trellix Insights: Turkish RAT Phishing Campaign.” *Trellixthrive*, 5 Aug. 2025, thrive.trellix.com/s/article/KB92580?language=en_US.

“2021 Turkey Threat Landscape Report (ENG).” *SOC Radar*, socradar.io/wp-content/uploads/2022/02/2021-Turkey-Threat-Landscape-Report-ENG.pdf. Accessed 10 Aug. 2025.