SECURITY COUNCIL

STUDY GUIDE

Aravali Model United Nations 2025

Agenda: Addressing the global threat posed by the Chinese hacking group ‘APT 41’ and its impact on increased geopolitical tensions and cyberterrorism globally

Freeze Date: 16th September 2020

Contents

Chairperson's Address

Greetings Delegates,

As your chairperson for Aravali Model United Nations 2025, it is my greatest honour to welcome you to the United Nations Security Council. It brings me immense pride to open our committee to one of the most pertinent and under-addressed challenges of our time - the rising threat posed by APT 41 and the increase in cyberterrorism globally.

Before I go into the complexities of the agenda, let me take a moment to reflect on the past few months, throughout which the Executive Board has worked tirelessly to bring this very committee to life. To us, this is not just a simulation - it is a space where diplomacy, critical thinking, and meaningful conversations can thrive. Innumerable hours have been poured into curating this agenda, which aims at building an experience that challenges each and every one of you to think as future leaders of the world. We've read all about firewalls, attribution mechanisms, zero-day vulnerabilities, Chinese threat actors - so that when you set foot into the room, the stage would be ready for diplomacy that matters.

Why does diplomacy matter, you may ask. It matters, because today, the battlefield is not just physical - it's digital. APT 41 is no longer just a hacker collective. It is a threat which is stealthy, borderless, and deeply destabilizing. It is the face of a new era of hybrid conflict, where the lines between statecraft and cybercrime blur. With cyberattacks targeting critical infrastructure such as health systems and government networks, the global security landscape is like nothing you have ever seen before. Hence, I call upon you, the Security Council, not only to respond to this untamed frontier, but to lead it and to emerge victorious.

This committee is more than just an academic exercise; it is a space for solutions. You represent the world's highest decision-making body which holds responsibility to craft real, impactful responses. It is the ideas you raise, the positions you defend, and the resolutions you craft, that is a testament to your commitment to global diplomacy.

I urge each of you to bring not only purpose and direction but also empathy to this room. Be assertive, be respectful, be creative, and most importantly, be open to new ideas. The challenges which we face today - much like cyber threats - are ever evolving. But so is our capacity to collaborate.

The future of the world might just depend on how we defend the invisible world of cyberspace. I look forward to a dynamic, diplomatic, and solutions-driven conference. The floor is now open.

Godspeed, delegates.

Aditri Chatterjee,

Chairperson,

United Nations Security Council.

(unsc.amun25@gmail.com)

Paperwork and AI Policy

The following forms of paperwork will be accepted in committee:

- Position Paper
- Directives
- Communiques
- Press Releases
- Presidential Statements
- Draft Resolutions

Position Paper

The significance of the Position Paper cannot be overstated as it is the first peace of paperwork that a delegate needs to submit. It should be submitted before the conference and gives the Executive Board a glimpse at the research done by the delegate and an overview of the delegate's portfolio.

A Position paper should ideally contain the following parts:

- Statement of Problem: Brief and general overview of the agenda from a neutral perspective, including the history of the problem, the possible causes, and the current state. It should cover all of the most important aspects of the situation from the delegate's perspective.
- Country Policy: It presents to the Executive Board how independent countries view the conflict. It should highlight the involvement of the country and any past actions taken by it regarding the agenda.
- Solutions: Solutions are the most important part of your position paper. It should give the executive board an idea of the unique and viable solutions you wish to pitch or implement during the committee. Furthermore, the first page of the Position Paper should be a cover page with the name of the committee, allotment, school, the names of the delegates and the agenda. The last page should be for Citations and the delegates are required to provide the executive board with the list of websites used by them in the making of the position paper.

Directives

This type of documentation is particularly helpful when the committee needs to act right away. Directives are broadly of two types with regards to the number of authors, and two types with regards to the number of viewers. Directives may be individual, i.e. from one delegate, or joint, i.e. from two or more delegates. They may also be covert, i.e. only

visible to the executive board or overt, i.e. visible to the whole committee. Directives typically contain a set of public instructions, or in certain situations, war plans, but they do not need to be formatted to the same extent as formal resolutions. In order for the delegates to employ directives as a tool to address the issues at hand, they are typically needed in committees following the introduction of many crises. However, all directives are subject to ratification by the Executive Board. The directive limit of the session/day and the status of the communication lines will be conveyed to the delegates once the session starts. 2 pre-committee directives will be accepted; these must be submitted to the committee email ID by 27th May 2025, 11:59 pm.

Communiques

As the name suggests, a communique is used as a means of communication to other people, within or outside the committee. Communiques are of two types - Public and Private and may be individually written or jointly written by 2 or more parties. Private communiques are sent to individual people and are for their eyes only. Public communiques, on the other hand, are used to make announcements to the entire committee, and anything written in a public communique is meant for the perusal of the entire committee. When it comes to communiques, creativity and originality are key. Communiques can be used to respond to updates in committee and the delegates can send a series of communiques if they wish to achieve a particular objective in committee. Communication lines will remain sporadically open throughout the course of the conference at the discretion of the Chairperson. The communique should be realistic and viable, they should be highly detailed. A covert communique need not follow international rules and regulations. Communique in response to an update will be highly favoured. Delegates are recommended to submit communique arcs to achieve a well thought out objective by the end of committee.

Press Release

Press Releases are tools used by committees or individuals to inform "the public" in the crisis about certain facts, or to spread misinformation about the ongoing crisis. Often, delegates may use these to try to influence public opinion against certain plans to help their own, to encourage the public to be safe, to stop protesting, or even to get involved with the crisis somehow.

Presidential Statement

A presidential Statement is an executive order issued by the Head of State. It is primarily used to announce a change or diversion from the normal foreign policy of a country that the delegate wishes the entire committee to know. It is also very important to not abuse the powers of a Presidential Statement. Any such paperwork which does not affect the

immediate flow of the committee or that which does not reflect a change in policy will not be ratified.

Draft Resolution

Draft Resolution is a formal document that specifies a plan of action that is to be undertaken by the United Nations Security Council to address a crisis. The Draft Resolution has an extremely strict format and not adhering to the format can get the resolution scrapped.

- A Draft resolution starts with a "name" or "title", followed by the names of the authors, then the signatories (delegates who wish for the resolution to be discussed in committee, not necessarily side with it) and finally enters the main body of the resolution.
- The main body of the resolution can also be subdivided into two parts, first are the preambulatory clauses [separator to be used is ","] and then the operative clauses [separator to be used is ";"]. Further, a full stop [.] signifies the end of the draft resolution.
- Authors: They are the members or countries who wish to introduce the paperwork written by them.
  Signatories: Are the members that want the paperwork to be discussed in committee. *Being a signatory does not imply that the member supports the resolution.*
- Phrases: Phrases are what we start clauses with. Preambulatory Phrases are phrases [have to be italicized] to start a preambulatory clause; Operative Phrase [have to be underlined] is to begin an operative clause.

NOTE:

All paperwork is subject to AI detection checks. The threshold for AI which is allowed is 15%. Any paperwork exceeding 15% AI will immediately be scrapped. All delegates are required to submit their paperwork only to unsc.amun25@gmail.com. Paperwork submitted on any other platform will not be accepted.

All paperwork must be submitted in PDF format with Garamond or Times New Roman, Size 12, Left Aligned Justified. All paperwork must follow this format: [Delegation] [Paperwork Type] [Operation Name (if applicable)].

Example: USA Directive Operation Hail Mary.

If the formatting is not followed delegates may be asked to reformat the paperwork and submit or have their paperwork scrapped altogether.

Only Position Papers are to be submitted on the given link: Position Papers

Position Papers submitted by mail will not be accepted.

Introduction to the United Nations Security Council

One of the United Nations six main bodies, the United Nations Security Council (UNSC) is in charge of safeguarding global security and peace, proposing new UN members for inclusion to the General Assembly, and approving any amendments to the UN Charter.

It has the authority to impose international sanctions, launch military operations, and form peacekeeping missions. The only UN body with the power to impose legally binding resolutions on member nations is the UNSC. Each of its fifteen members has one vote. According to the United Nations Charter, all Members are required to abide with Council decisions. Five of the fifteen members of the Security Council—China, France, Russia, the United Kingdom, and the United States—are permanent members.

Any substantive Security Council resolution is subject to the veto (blocking) power of the permanent members. This veto power does not apply to any votes or matters that come before the General Assembly or emergency special sessions of the General Assembly. The remaining ten members are chosen regionally and serve two-year terms. The group's members alternate monthly holding the presidency.

When determining whether there is a violation or imminent danger to the peace, the Security Council is in charge. It suggests ways of altering the terms of settlement and encourages parties to a conflict to settle it peacefully. The Security Council occasionally has the option of using sanctions or even approving the use of force in order to preserve or restore global peace and security. Article 30 of the Charter stipulates that the Security Council shall adopt its own rules of procedure, and in 1946, the council adopted its Provisional Rules of Procedure(S/96). Subsequently, the Provisional Rules of Procedure were modified on several occasions; the last revision was made in 1982(S/96/Rev.7) in order to add Arabic as the sixth official language, in conformity with General Assembly resolution 35/219 of 17 December 1980.

Functions

Under the United Nations Charter, the functions and powers of the Security Council are:

- to maintain international peace and security in accordance with the principles and purposes of the United Nations;
- to investigate any dispute or situation which might lead to international friction;
- to recommend methods of adjusting such disputes or the terms of settlement;
- to formulate plans for the establishment of a system to regulate armaments;
- to determine the existence of a threat to the peace or act of aggression and to recommend what action should be taken;
- to call on Members to apply economic sanctions and other measures not involving the use of force to prevent or stop aggression;
- to take military action against an aggressor;
- to recommend the admission of new Members;

- to exercise the trusteeship functions of the United Nations in "strategic areas";
- to recommend to the General Assembly the appointment of the Secretary-General and, together with the Assembly, to elect the Judges of the International Court of Justice.

Mandate

The United Nations Charter established six main organs of the United Nations, including the Security Council. It gives primary responsibility for maintaining international peace and security to the Security Council, which may meet whenever peace is threatened. According to the Charter, the United Nations has four purposes:

- to maintain international peace and security;
- to develop friendly relations among nations;
- to cooperate in solving international problems and in promoting respect for human rights;
- and to be a centre for harmonising the actions of nations.

All members of the United Nations agree to accept and carry out the decisions of the Security Council. While other organs of the United Nations make recommendations to member states, only the Security Council has the power to make decisions that member states are then obligated to implement under the Charter.

When a complaint concerning a threat to peace is brought before it, the Council's first action is usually to recommend that the parties try to reach agreement by peaceful means. The Council may:

- set forth principles for such an agreement;
- undertake investigation and mediation, in some cases;
- dispatch a mission;
- appoint special envoys; or
- request the Secretary-General to use his good offices to achieve a pacific settlement of the dispute.

When a dispute leads to hostilities, the Council's primary concern is to bring them to an end as soon as possible. In that case, the Council may:

- issue ceasefire directives that can help prevent an escalation of the conflict;
- dispatch military observers or a peacekeeping force to help reduce tensions, separate opposing forces, and establish a calm in which peaceful settlements may be sought.

Beyond this, the Council may opt for enforcement measures, including:

- economic sanctions, arms embargoes, financial penalties and restrictions, and travel bans;

- severance of diplomatic relations;
- blockade;
- or even collective military action.

The primary goal is to aim at those liable for the international community's condemned policies or practices while minimizing the repercussions of the actions taken on other segments of the population and the economy.

Delegates are requested to visit the given link for more information on the UNSC and its work:

https://www.un.org/securitycouncil

Detailed Timeline of Attacks

1. **2012–2014:** APT41 first appears (tracked since ~2012) conducting intrusions in China (e.g. hotel networks for state guests) and on technology and gaming companies. By 2014 it had split into dual campaigns: simultaneous cyber espionage and financially-motivated attacks. During this period the group was especially active in video game companies, using supply-chain malware (Winnti/PlugX) to steal source code, certificates, and virtual currency.

2. **2014–2018:** The group continued broad espionage. It infiltrated high-tech and telecom firms (e.g. stealing call-records from telco databases), and targeted healthcare and research: e.g. it compromised medical device/software companies and even U.S. cancer research labs. APT41 also engaged in cybercrime for profit (crypto-mining, ransomware) alongside state tasks.

3. **Aug 15, 2019**: First U.S. indictment of APT41 members. A federal grand jury in Washington charged two Chengdu-based hackers – Zhang Haoran and Tan Dailin – with intrusions into dozens of U.S. and UK companies (especially high-tech and video game firms). They were charged with unauthorized access and attempted extortion after deploying malware at companies including a gaming software producer and a UK resident's site.

4. **Jan 20 – Mar 11, 2020:** Global exploitation campaign. Mandiant observed APT41 exploiting multiple unpatched enterprise vulnerabilities worldwid. Beginning Jan 20, 2020, they ran mass scans and intrusions via Citrix ADC (CVE-2019-19781) on ~hundreds of servers, and on Jan 21 deployed web shells (e.g. China Chopper) to drop Cobalt Strike BEACON backdoors on many organizations. Concurrently they exploited Cisco RV320/RV325 router flaws (CVE-2019-1652/1653) to compromise a telecommunications provider on Feb 21 (delivering an ELF backdoor "fuc"). In mid-February they also exploited a Zoho ManageEngine zero-day (CVE-2020-10189) to breach at least five customers. Targets spanned banking/finance, government, healthcare, telecom, manufacturing, and education across 20+ countries (USA, India, UK, Saudi Arabia, etc.). These intrusions installed persistent backdoors (custom web shells and Cobalt Strike) for ongoing access.

5. **July 21, 2020:** DOJ indicts two MSS-linked APT41 hackers. In Spokane, WA the U.S. unsealed charges against Li Xiaoyu and Dong Jiazhi, accusing them of a decade-long intrusion campaign. The indictment alleged they stole terabytes of confidential data from 100+ companies in sectors like tech manufacturing, medical devices, pharmaceuticals, civil engineering and video gaming. (They even targeted companies developing COVID-19 vaccines, then tried to extort payment for the stolen code.) The defendants were identified as Ministry of State Security

officers. Outcome: charged with conspiracy, computer hacking, and attempted extortion.

6. **Aug 11, 2020:** DOJ indicts three Chengdu 404 Network Technology hackers (Qian Chuan, Fu Qiang, Jiang Lizhi) in DC. These APT41 operatives were charged with racketeering and conspiracies for "supply-chain" intrusions: they hacked software publishers to implant malware in legitimate updates. Victims included social media, telecommunications, government, defense, and university networks. The scheme affected hundreds of companies in Australia, Brazil, Germany, India, Japan, Sweden, etc. They used spear-phishing and third-party VPN tools for initial access, and deployed ransomware/cryptominers after stealing credentials.

7. **Aug 2020:** Video-game conspiracy indictment. In the same grand-jury action, DOJ charged two Malaysian businessmen with working with the Chinese hackers to profit from intrusions into the video game industry (injecting code to steal game currency). U.S. authorities issued arrest warrants; indeed two conspirators were arrested in Malaysia in Sept 2020.

8. **Sep 14–16, 2020:** US DOJ and FBI publicly attribute these operations to "APT41". The DOJ press release (Sep 16) announced charges against 7 defendants (5 Chinese hackers and 2 foreign co-conspirators) for intrusions into over 100 organizations worldwide. DOJ noted APT41 had compromised software, hardware, telecom, and game companies to steal intellectual property and account data. U.S. law enforcement (FBI/CISA) issued technical alerts and worked with partners to freeze APT41 infrastructure and prevent further access.

Sectoral Impacts

- **Healthcare & Pharma:** APT41 has repeatedly targeted healthcare and biotech organizations. Between 2014–2020 they conducted campaigns against medical device/software firms, biotech companies, and even U.S. cancer research facilities. In 2020 they breached hospitals and research centers, including those working on COVID-19 vaccines. By stealing research data and R&D secrets, APT41 undermines medical innovation and public health preparedness (although no mass patient data leaks are publicly reported). U.S. agencies now warn that Chinese APTs like APT41 pose a "significant threat to the healthcare and pharmaceutical industries".
- **Telecommunications:** Multiple APT41 operations have directly hit telecom infrastructure. For example, in early 2020 they installed malware on Cisco routers in a telecom company. The FBI also reported that APT41 targeted telecom providers in India, Pakistan, South Korea, Taiwan and other nations. They have stolen call-detail records from carrier networks and compromised networking equipment to intercept or reroute communications. Disruption of telecom systems could compromise customer privacy and critical communications.
- **Finance:** The group has pursued financial gain through its hacks. They attacked banks and financial service firms (spear-phishing executives and infiltrating back-end systems). APT41 deployed crypto-mining malware ("cryptojacking") on victim servers and attempted ransomware extortion. Notably, DOJ reported they tried to ransom stolen source code and certificates by demanding payment in cryptocurrency. Such attacks impose direct monetary losses on companies and threaten economic stability.
- **Government, Defense & Civil Society:** APT41 has spied on foreign governments and nonprofit groups. The FBI notes they targeted government agencies, think tanks, and activists globally. DOJ specifically cited theft of data from pro-democracy organizations in Hong Kong and dissidents. By stealing policy documents, negotiations, and personal data from civil society, APT41 advances Chinese state interests and undermines democratic processes. In one example, Chinese targets (e.g. Hong Kong activists) saw APT41 hacks facilitating surveillance and intimidation of dissenters.
- **Technology & Manufacturing:** High-tech companies and manufacturers have suffered major losses. APT41's hallmark has been supply-chain compromises of software and hardware. They stole source code and proprietary designs from tech firms, and even harvested digital certificates to sign malware as if it were legitimate. The gaming industry was heavily hit: APT41 secretly altered video-game server software to skim virtual currency. In technology manufacturing (semiconductors, electronics, communications hardware), APT41 exfiltrated intellectual property to give Chinese firms an economic edge. The cumulative effect is to rob companies of competitive advantage and, in national security terms, to compromise defense supply chains.

Relevant International Cyberterrorism Attacks

- **Russia (State-sponsored):** Russia's GRU/FSB launched several high-impact attacks. In 2017, the NotPetya malware (spread via a Ukrainian accounting software) paralyzed systems globally (transport, energy, finance, healthcare) and has been attributed to Russian military actors. Russian APT28/29 also famously hacked political organizations in the U.S. (2016 election interference) and Europe (e.g. German parliament in 2015, French election servers in 2017). In 2018–2020, Russia continued cyber espionage: for example, Fancy Bear targeted U.S. state governments and NATO agencies, and in 2020 Russian GRU officers were indicted for past hacks on Ukraine and US infrastructure. (These incidents show the global scope of Russian cyber campaigns, which often aim at military/political intelligence and disruption.)
- **North Korea (State-sponsored):** North Korea's Lazarus Group carried out the 2017 WannaCry ransomware attack, which infected over 300,000 computers in 150+ countries, crippling hospitals and businesses. It also conducted the 2014 Sony Pictures hack (retaliation for a film) and the 2016 Bangladesh Bank SWIFT heist ($81M theft). In 2020 the U.S. indicted Lazarus affiliates for cybercrimes including targeting cryptocurrency firms worldwide. North Korea's attacks often blend financial crime (to fund the regime) with disruptive "cyber warfare."
- **Iran (State-sponsored):** Iranian hackers (linked to the IRGC's Cyber Command and other agencies) have executed espionage and sabotage campaigns. In 2012–2016 Iran was blamed for industrial malware (like Shamoon on Saudi oil facilities). By 2018–2020, Iran's APT33/34 groups targeted aviation, energy and political organizations in the Middle East and West. In September 2020 the U.S. indicted three IRGC-affiliated hackers for targeting aerospace companies and government organizations. Iranian operations often serve both intelligence-gathering and revenge (e.g. against dissidents). (The Carnegie and CSIS reports emphasize that Iranian cyber operations are "among the most sophisticated, costly, and consequential" globally.)
- **Non-State/Hacktivist Groups:** Various non-state actors (hacktivists, cybercriminals, terrorist sympathizers) have also conducted cyberattacks, though usually smaller in scale than nation-state campaigns. For example, hacktivist groups like Anonymous targeted ISIS social media in 2015, or Russian-linked hacktivists defaced websites during conflicts. Terrorist organizations (ISIS, Al-Qaeda) have used social media and encrypted messaging aggressively, but their actual cyberattacks have been mostly propaganda or simple hacks. The 2010s also saw a boom in cybercrime (ransomware gangs like WannaCry, NotPetya, and later Maze/Conti, targeting hospitals and critical infrastructure for profit). While financially motivated, these ransomware campaigns (LockBit, REvil, etc.) caused widespread disruption (notably affecting hospitals, city services, and companies from 2018–2020).

- **Other Notable Incidents:** There were many other notable breaches: for example, the 2010s' U.S. Office of Personnel Management breach (theft of 22 million records by Chinese APT1), the 2017 Ukrainian power grid attack (Russia), and intrusions into the 2020 US Census Bureau and COVID vaccine researchers (attributed variously to Russia, China, Iran). In each case, like with APT41, governments cited the importance of attribution and international norms in holding perpetrators accountable.

Related topics to cover in Committee

Cybercrime and Human Security

In an address to the Commission on Crime Prevention and Criminal Justice (CCPCJ) in 2018, Secretary-General Antonio Gutterres stated that "cybercrime is an area in which there is much work to do and no time to waste… The online sexual exploitation and abuse of children is proliferating, and women and girls are disproportionately harmed." Cybercrime notoriously lacks an internationally recognized definition, but the United Nations Office on Drugs and Crime (UNODC) notes that "broadly, cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse." The UNODC elaborates that "perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic, and international response." Cybercrime is a novel, pressing threat to both international and state security; however, this committee will address not just these risks, but the risks placed on human security as well. As per General Assembly resolution 66/290, human security is defined as "an approach to assist Member States in identifying and addressing widespread and cross-cutting challenges to the survival, livelihood and dignity of their people." It further notes that "human security calls for people-centred, comprehensive, context-specific and prevention-oriented responses that strengthen the protection and empowerment of all people." In their 2023 Summary Report, the Internet Governance Forum (IGF) emphasized the challenges posed in constructing policy that both curbs the threats to human security posed by cybercrimes while avoiding encroaching on civil liberties and human rights. Bear this in mind as you begin considering responses to the ever-evolving threat posed by cybercrime.

In 2019, the General Assembly successfully passed resolution 74/247 on "Countering the use of information and communications technologies for criminal purposes." This document set in motion a years-long process of negotiation for a treaty on cybercrime, one that is still yet to be completed. It further established an intergovernmental ad hoc committee to prepare this treaty, one chaired by H.E. Ms. Faouzia Boumaiza Mebarki from Algeria, and composed of an "intergovernmental committee of experts [and] representative of all regions." This committee has engaged in eight sessions since its inception (6 main, 2 organizational), and its final session will conclude on February 9th, 2024. While a formal agreement on cybercrime is yet to be fully realized, a firm groundwork has been laid. As early as 2012, the Human Rights Council passed resolution 20/L.13, calling for the recognition of the internet as a theatre for both the realization and stifling of the human right to freedom of expression. Security Council resolutions 2178 (2014) and 2396 (2017) both set forth a mandate for Member States to engage collaboratively to counter terrorist efforts in abusing technology. The UNSC Counter Terrorism Committee (CTC) further unanimously adopted the Delhi Declaration, which committed Member States "to prevent and combat digital forms of terror, notably using drones, social media, and online terrorist financing." Furthermore, efforts have also been

made at establishing capacity-building initiatives targeted squarely at cybercrime and cybersecurity. For example, the United Nations Office of Counter-Terrorism (UNOCT) has worked diligently in the realm of cybersecurity to improve the resilience of all Member States to cybercrime. UNOCT has launched such initiatives as the Cybersecurity and New Technologies programme. This program bears four primary goals: Developing knowledge and raising awareness of challenges and opportunities related to new technologies in countering terrorism; Enhancing skills and capacities required to develop and implement effective national counter-terrorism policy responses to the challenges and opportunities of new technologies; Enhancing skills and capacities required to protect critical infrastructures against terrorist cyber-attacks; and Enhancing criminal justice capacities to counter and investigate terrorist use of new technologies. Through programs such as this, Member States are supported in their endeavours to maintain both state and human security from threats posed by cybercrime, while also being able to actively pursue perpetrators.

With the onset of the COVID-19 pandemic the world saw an exponential amount of people connected to the internet. In the United States (US) alone there were 800,944 complaints of cybercrimes with a net loss amount of $10.3 billion in 2022, according to the FBI. Though there was a decrease of 5% in the number of complaints, there was also a 49% increase in the dollar losses experienced. Of the crimes committed, phishing schemes were the most reported with 300,497 complaints with a total of $52 million in losses. In regard to financial losses, with a total of $3.3 billion in losses, investment schemes take the cake. The largest demographic to report cybercrime were those between the ages of 30 and 39, but the greatest dollar loss was experienced by those in the 60+ range. Interestingly enough, cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in losses with those between 30 and 49 being the most targeted. The US, however, wasn't the only nation afflicted with an onslaught of cybercrimes. Another nation heavily attacked was India. According to Statista, there were 27,374 arrests nationwide in India for those committing cyber crimes in 2023. The most common crime committed was multipurpose malware, or software designed to harm multiple facets of a target's software. 52,000 crimes were committed in 2023 with a total accumulation of $2.18 million in damages. Another country that has been a hotspot for cybercrimes was Russia. In 2021, Russia accounted for a quarter of all unsolicited spam emails sent to persons, in one day alone that year more than 7 billion spam emails were sent from Russia according to Statista. Though, also in 2021, 18% of personal computers faced at least one malware attack and one-tenth of all computers in Russia were attacked by phishing schemes on a yearly basis. Other nations, such as those in Latin America, have faced some serious damages from cybercrimes as well. In 2019, Ecuador and Paraguay saw the most cyberattacks than any country in the region with 70% of their IT managers reporting malware infections. Brazil, Colombia, and Mexico account for 9 out of 10 attacks registered in Latin America combined, according to Statista. 65% of cyberattacks reported in 2020 in Brazil were ransomware attacks, it's the same case for Colombia and Mexico but at 44% of crimes reported. That being said the Brazilian, Colombian, and Mexican governments have taken some steps to prevent these crimes being committed. Colombia has the highest percentage of companies with cybersecurity

politics and all three nations have their IT teams spend exorbitant amounts of time on security. However, the three spend at least a third of their time responding to cyberattacks.

The UN has taken many steps in the effort to curtail the effect of cyberattacks and to bolster the development of cybersecurity. One of the first actions taken to curb cyberattacks was Resolution 55/63, adopted in January 2001. In this resolution, the UN recognizes the need to combat the criminal misuse of information technologies. That the development of free flow technologies and telecommunications can promote economic and social development, education, and democratic governance. However, it also recognizes that there is a concern in these advancements that may create new opportunities for criminal misuse and activity. The resolution also gives credit to the Council of Europe, Group of Eight (at the time), and the Organization of American States and their subsidiary bodies for putting effort into the prevention of criminal misuse of information technologies. It also notes that Member States should update their laws to prevent criminal misuse of these new technologies as well as ensuring cooperation between Member States and their law enforcement agencies in the prosecution of those that commit cyber crimes. That Member States legal systems should also be updated to ensure the safety and protection of data that may be breached. Another resolution enacted by the UN is Resolution 57/239 that was passed in January 2003. This resolution calls for the creation of a global culture of cybersecurity. In its call for the creation of a global culture, the UN, in this resolution, recalls previous resolutions such as Res. 55/63. It also notes the growing dependence on information technologies and that with increased usage of these technologies there must be an increase in cybersecurity provided, that effective cybersecurity isn't guaranteed by governments or law enforcement, but also through prevention and societal support. That it is pertinent that all parties that use this technology, whether it be governments, organizations, or private owners or users, must be aptly informed of necessary cybersecurity measures to prevent and combat criminal misuse. It acknowledges that gaps in the access to and use of these technologies by Member States can greatly impair the effectiveness of international cooperation in combating criminal activity. The aforementioned resolution also notates the elements needed to create a global culture of cybersecurity. The resolution labels those that utilize information technologies as "participants." This includes governments, businesses, other organizations, and individuals. It highlights that participants should be aware of the need for security, that they are responsible for the security of their systems, and that they should respond in a timely manner to prevent, detect security incidents. It also stressed that participants should act in a manner that is ethical and should routinely conduct risk assessments to their systems. That they must design and implement, as well as manage the security used in their systems. Participants should also assess the security of their systems as well. Ultimately though, security should be implemented in a manner that is in accordance with democratic principles. Resolution 58/199 passed by the UN General Assembly (UNGA) in March 2010 was adopted to create a global culture of cybersecurity and to protect critical information infrastructures. This resolution recognizes the newfound reliance of information technologies in business sectors such as the generation, transmission, and distribution of energy, or banking and financial

services, to name a few. It acknowledges that for the effective protection of systems there is a required communication and cooperation nationally and internationally amongst all parties that are involved. The resolution highlights the elements needed to protect the critical information infrastructures of those it concerns. Such elements include having emergency warning systems to alert one of cyber threats. Raise awareness to help those involved in their understanding of these infrastructures and the role each plays. Examine the infrastructures and identify any dependencies to help enhance their protection. Promote partnership, both public and private, to share and analyze these systems to prevent, investigate and respond to damage or attacks on such infrastructures. Carry out the training and exercises necessary to enhance the response capabilities as well as have adequate substantive and procedural laws and trained personnel to enable Member States the ability to investigate and prosecute attacks on critical information.

State Sponsored Cyberterrorism

In the evolving landscape of global security threats, state-sponsored terrorism has increasingly taken root in the digital realm, leveraging cyberspace and advanced technologies to conduct covert operations that destabilize rival nations, disrupt critical infrastructure, and sow fear among civilian populations. Unlike traditional forms of terrorism, state-sponsored cyberterrorism often blurs the lines between espionage, sabotage, and warfare. Nations such as Russia, China, Iran, North Korea, and even technologically advanced democracies like the United States and Israel have developed sophisticated cyber capabilities used not only for surveillance but also for active disruption. High-profile incidents, such as the U.S.-Israel developed *Stuxnet* virus targeting Iranian nuclear facilities, Russia's alleged cyber interference in foreign elections, and North Korea's Lazarus Group conducting financial heists to fund weapons programs, reflect a growing trend where states employ digital tools to achieve geopolitical objectives through asymmetric, deniable means.

Cyberterrorism as an extension of state policy is especially dangerous due to its scalability, low entry barriers, and anonymity. Governments have increasingly turned to third-party cybercriminals, hacktivist groups, or state-backed advanced persistent threats (APTs) to wage digital warfare without direct attribution. These actors exploit vulnerabilities in public infrastructure, financial systems, energy grids, and health sectors—undermining national stability and public trust. The dark web has further enabled these activities by providing platforms for malware distribution, data laundering, and hiring of "cybercrime-as-a-service" agents, creating a transnational ecosystem of illicit collaboration between state and non-state actors.

In response to these rapidly escalating threats, the United Nations has begun playing a more proactive role in coordinating international countermeasures. The United Nations Security Council (UNSC) has increasingly addressed cyberterrorism through informal briefings and formal statements, acknowledging the implications of state-sponsored cyberattacks for global peace and security. A notable development was the April 2024 Arria-formula meeting, which brought together member states and UN agencies to

discuss digital threats and propose norms to govern state behavior in cyberspace. This was particularly significant in linking cyberterrorism to Article 39 of the UN Charter, which permits the Council to address threats to international peace.

Furthermore, the United Nations Office of Counter-Terrorism (UNOCT), along with its Centre for Counter-Terrorism (UNCCT), has launched several initiatives under its "Cybersecurity and New Technologies" program. These include simulations, training exercises, dark web forensics, and capacity-building workshops that enhance the ability of member states—particularly developing nations—to detect, investigate, and respond to cyber-enabled terrorism. In partnership with the UN Interregional Crime and Justice Research Institute (UNICRI), the UN has also produced groundbreaking research like the "Beneath the Surface" report, which analyzes how state-linked terrorist groups exploit digital platforms and anonymized technologies.

Alongside these efforts, the UN is actively promoting treaty negotiations through the Ad Hoc Committee on Cybercrime, with the aim of establishing a universal legal framework that clearly defines cyberterrorism, sets standards for state accountability, and enables international cooperation in investigation and prosecution. However, consensus has been difficult to achieve due to differing interpretations of data sovereignty, cyber warfare, and human rights protections. Developed and developing countries often find themselves at odds over surveillance concerns, evidentiary standards, and digital freedoms.

Complementing its policy and legal work, the UN also supports global coordination through multilateral platforms like the International Multilateral Partnership Against Cyber Threats (IMPACT), under the ITU. This body facilitates real-time cyber incident monitoring and response across over 150 member states and encourages public-private partnerships critical for rapid innovation and threat mitigation. These collaborative frameworks are essential in a world where cyber operations increasingly cross national borders and require joint, swift, and transparent action.

Despite these initiatives, significant challenges remain. The problem of attribution continues to hinder accountability, as state actors often operate through proxies or anonymizing technologies that complicate investigation. Moreover, there are wide gaps in cybersecurity infrastructure, legislation, and technical capacity between developed and developing countries—making the latter disproportionately vulnerable. The ever-evolving nature of cyber tools, such as AI, deepfakes, IoT exploits, and drone-borne cyber attacks, further expands the threat matrix, demanding continuous adaptation and foresight.

In conclusion, the intersection of state-sponsored terrorism, cyberspace, and emerging technology represents one of the most pressing global security threats of the 21st century. The United Nations, through its diverse agencies and diplomatic mechanisms, plays a critical and evolving role in addressing these threats. While progress is evident in the form of policy dialogue, capacity-building, and treaty negotiation, the future effectiveness of the UN's response will hinge on its ability to foster international consensus, ensure equitable access to cyber defense resources, and embed cyber norms within a framework that respects both sovereignty and human rights. As cyberwarfare

grows more normalized and sophisticated, the UN's leadership in this domain is not just beneficial—it is essential.

Relevance of the Freeze Date

The September 16, 2020 U.S. Department of Justice (DOJ) announcement attributing cyberattacks to APT41 had far-reaching geopolitical, cybersecurity, and diplomatic implications. The unsealing of indictments against five Chinese nationals and two Malaysian accomplices marked one of the most comprehensive and public legal actions against a state-linked Advanced Persistent Threat (APT) group to date. By explicitly naming APT41 and linking it to the Chinese state—even while noting their actions also served personal financial interests—the U.S. reinforced the narrative of China as a hybrid cyber actor, capable of blending state-sponsored espionage with cybercriminal activity.

- Cybersecurity Implications:
  The announcement heightened urgency across public and private sectors to identify and mitigate APT41's tactics, techniques, and procedures (TTPs). The FBI and CISA released detailed technical alerts, providing Indicators of Compromise (IOCs), malware signatures, and attack vectors, which helped organizations worldwide patch vulnerabilities and shore up defenses. These alerts particularly focused on supply chain infiltration, web shell deployments, and credential theft in telecom, tech, healthcare, and educational sectors. Additionally, APT41 infrastructure was reportedly frozen or dismantled, making this one of the few instances where attribution was accompanied by visible operational disruption. This move sent a strong message that the U.S. would act not only through diplomacy but also technical means to degrade adversarial cyber capacity.

- Geopolitical & Legal Implications:
  The DOJ's strategy of "naming and shaming" also had diplomatic consequences, intensifying tensions between the United States and China. It contributed to an emerging doctrine in which legal indictments become tools of foreign policy—signaling that cyber aggression would be met not only with countermeasures but with international legal accountability. The move also pressured China's global image, exposing its clandestine operations and undermining claims of "non-interference." The inclusion of foreign co-conspirators further illustrated the transnational nature of cybercrime, showing how state actors often work with private contractors or criminal proxies to evade detection and scale operations.

- International Cooperation & Precedent Setting:
  This action also catalyzed greater international collaboration, as U.S. authorities worked with foreign governments—including those in Southeast Asia and Europe—to arrest, extradite, and neutralize threat actors. It helped set a legal and strategic precedent for future indictments against nation-state hackers, laying the groundwork for global frameworks that address cyber attribution and accountability. Moreover, it encouraged allied nations to increase investment in cyber forensics, attribution capabilities, and law enforcement modernization.

- Strategic Messaging to the Private Sector:
  For corporations, especially in industries like software development, telecom, gaming, and healthcare, the event highlighted the vital importance of cybersecurity hygiene, threat intelligence sharing, and supply chain risk management. The fact that APT41 targeted companies for both espionage and monetization revealed the need for holistic defense strategies that go beyond protecting intellectual property to include account data, infrastructure, and third-party software.

Major Parties Involved

1. United States of America

   The United States was arguably the most heavily targeted and impacted country by APT41. Over 100 American companies, government agencies, and academic institutions were compromised across industries like healthcare, telecommunications, defense, software, and education. The group's activities included the theft of intellectual property, personal data, and credentials, as well as espionage against public institutions. The U.S. responded robustly: the Department of Justice (DOJ) unsealed indictments on September 16, 2020, against five Chinese hackers and two Malaysian collaborators, marking one of the most public legal responses to state-linked cybercrime. Additionally, the FBI and CISA issued technical alerts, and the U.S. worked with international partners to freeze APT41 infrastructure, disrupting their operations. These events deepened cybersecurity preparedness across American industries and triggered stronger advocacy for global cyber norms.

2. China

   Ironically, China—despite being the origin country of APT41—was affected in more indirect but profound ways. The public attribution of APT41 as a Chinese state-sponsored group strained diplomatic relations between China and the United States. While Beijing denied the allegations and claimed it opposes all forms of cybercrime, the indictments added to a growing body of evidence suggesting China uses third-party cyber actors for deniable operations. Internally, it is likely the exposure led to increased secrecy and reorganization among China's cyber units. The fallout also pushed China to double down on cyber sovereignty narratives, pushing back against Western-led cyber governance frameworks.

3. Russia

   While Russia was not a primary target of APT41, the two countries share similarities in their use of state-aligned hacking groups for asymmetric advantage. Russia likely observed the APT41 case closely, particularly how the U.S. handled public attribution and technical countermeasures. Strategically, Russia may have adapted its operational security models in response to the visibility of APT41's compromise. Some Russian institutions could have been incidentally affected through software supply chains or global platforms breached by APT41, although there is no direct public evidence of focused targeting.

4. North Korea

North Korea was also not a direct target, but as a fellow state engaged in state-sponsored cyber operations—through groups like Lazarus Group—it found itself indirectly involved in the global conversation about cybercrime. North Korea, much like Russia and China, has exploited similar methods such as spear phishing, cryptocurrency theft, and software vulnerabilities. The exposure of APT41 may have pressured North Korea to reassess its own attribution risks and led to more refined use of third-party proxies or infrastructure.

5. South Korea

South Korea was significantly affected due to its close ties with the U.S. and its advanced tech ecosystem. APT41 targeted telecoms, gaming companies, and software vendors, sectors in which South Korea is globally dominant. Intellectual property theft and user data breaches raised alarms among South Korean corporations. As a result, Seoul strengthened its national cybersecurity posture, deepened collaboration with the U.S. on cyber defense, and issued industry-specific advisories to mitigate persistent Chinese-origin cyber threats.

6. Taiwan

Taiwan has long been a critical geopolitical and cyber target for Chinese-affiliated APTs. APT41 specifically targeted Taiwanese semiconductor firms, defense contractors, and telecom companies, aiming to extract both commercial secrets and sensitive communications. Given the intense cross-strait tensions, these attacks were viewed as extensions of Chinese strategic pressure in cyberspace. Taiwan responded by enhancing its national CERT (Computer Emergency Response Team) capabilities and increasing international cooperation, particularly with the U.S. and Japan, to defend against advanced cyber threats.

7. India

India, being a strategic and regional rival to China, was a frequent target of cyber intrusions, particularly in the telecom, pharmaceutical, and critical infrastructure sectors. By 2020, APT41 had exploited vulnerabilities in Indian systems (such as Citrix and Pulse Secure VPNs), accessing internal networks to exfiltrate data. Indian IT services firms and government-linked contractors were targeted, with concerns over data theft, surveillance, and supply chain manipulation. The intrusions also deepened cybersecurity anxieties during a time of rising border tensions in Ladakh, prompting Indian agencies to accelerate cyber defense initiatives and collaborate more closely with the U.S. and Quad nations on cyber intelligence.

8. Vietnam

Vietnam's growing tech and manufacturing sectors made it an appealing target for APT41. Reports suggested that Vietnamese telecommunications firms, public sector databases, and logistics companies were among the victims. Given the country's increasing strategic distance from China and closer alignment with the U.S., these intrusions were interpreted as efforts to monitor political intentions and access economic insights. Vietnam, like India, faced espionage-style threats rather than overt financial targeting, though public disclosure was limited due to government opacity on cybersecurity incidents.

9. Australia

Australia was heavily affected, especially in its health, education, and technology sectors. Universities and research institutions were frequent targets—likely related to COVID-19 vaccine and health data espionage. APT41's known exploitation of software supply chains raised alarm bells in Australia, particularly after the Australian Cyber Security Centre (ACSC) confirmed frequent Chinese-origin attacks on national infrastructure. Australia responded with new cybersecurity funding, public attribution policies, and diplomatic warnings, placing APT41's activity within the broader context of deteriorating Sino-Australian relations.

10. Japan

Japan, a key ally of the U.S. and a tech leader, was impacted via intrusions into gaming companies, defense contractors, and electronics manufacturers. APT41's targeting of Japanese companies appeared to be industrial espionage, aimed at harvesting R&D data, technology blueprints, and user credentials. The attacks exposed vulnerabilities in Japanese cybersecurity practices, especially among midsize companies, and pushed Japan to increase national investment in threat detection and public-private cyber cooperation. Though Japan did not publicly attribute attacks to APT41 at the time, internal awareness of Chinese-origin threats grew substantially.

11. United Kingdom

The United Kingdom experienced indirect and direct consequences of APT41 operations. British healthcare entities, pharmaceutical research firms, and academic institutions conducting COVID-19 research were reportedly targeted. Additionally, British software vendors and cloud service providers used globally were part of the broader APT41 supply-chain compromise strategy. Although the UK did not specifically name APT41 in early statements, intelligence agencies like GCHQ increased alerts around Chinese

state-sponsored threats and engaged in joint attribution efforts with the U.S., signaling close coordination behind the scenes.

12. Germany

Germany was targeted mainly through technology and automotive supply chains, areas central to its economy. APT41 used sophisticated backdoors and remote access tools to infiltrate IT systems of German firms connected to advanced engineering, telecom infrastructure, and pharmaceuticals. Given Germany's leadership role in the EU, these intrusions were likely part of strategic intelligence gathering. The Federal Office for Information Security (BSI) was involved in quiet mitigation efforts and began pushing for tighter software security regulations in response.

Emerging Global Challenges

1. Blurring of Lines Between State and Criminal Actors
   APT41's operations exemplified a dangerous hybrid model—where hackers were allegedly linked to Chinese state intelligence but also engaged in financially motivated cybercrime. This dual-use strategy blurred traditional lines between espionage and criminal activity, making attribution, legal recourse, and retaliation far more complex. Governments now faced the challenge of addressing threats that were both state-backed and profit-driven, creating legal and strategic ambiguity.

2. Fragility of Global Supply Chains and Infrastructure
   APT41 exploited software vulnerabilities and supply-chain weaknesses to infiltrate major companies and institutions. Their ability to implant web shells, backdoors, and trojans in commonly used applications revealed the fragility of global digital infrastructure, especially in cloud services, enterprise software, and managed service providers. As the pandemic forced more businesses online in 2020, the attacks underscored how interconnected yet vulnerable the global cyber ecosystem had become.

3. Ineffectiveness of Existing Legal Norms and Enforcement

   Despite detailed indictments and technical attribution, the likelihood of apprehending or extraditing APT41 members remained slim. The legal mechanisms of international law—particularly regarding cybercrime—proved insufficient, slow, and unenforceable against state-sponsored actors operating from protected jurisdictions. This posed a major challenge for justice systems and highlighted the urgent need for global treaties and extradition norms in cyber governance.

4. Erosion of Trust in Cyberspace
   APT41's broad range of targets—including healthcare providers, educational institutions, defense contractors, and game companies—demonstrated that no sector was immune. The attacks shook public trust in digital platforms, especially those involving personal data, intellectual property, or critical services. This loss of trust led to calls for greater digital transparency, public-private threat sharing, and regulatory oversight.

5. Escalating Geopolitical Tensions and Cyber Attribution
   The U.S. decision to publicly attribute the attacks to China, and to unseal indictments, intensified an already deteriorating U.S.–China relationship. It

introduced a new era of cyber-diplomatic confrontation, where states began treating cyber intrusions as public acts of aggression. This shift forced many nations to reconsider their cyber deterrence doctrines, invest in attribution capabilities, and prepare for cyber escalation scenarios in both diplomatic and military settings.

6. Rising Demand for International Cyber Cooperation
   APT41's operations—spanning over 100 victims in more than a dozen countries—demonstrated that cyber threats were borderless. This prompted renewed calls for international cooperation on cybersecurity through forums like the United Nations, INTERPOL, and the Budapest Convention on Cybercrime. However, political divisions—especially between authoritarian and democratic regimes—hampered progress on shared definitions, accountability, and enforcement mechanisms.

7. Cybersecurity Gaps in Developing and Middle-Income Countries

   While major economies were able to detect and respond to APT41's attacks, developing countries often lacked the infrastructure, expertise, and resources to defend themselves or recover quickly. This widened the global cybersecurity inequality, exposing how some regions could become silent victims of large-scale cyber campaigns. Strengthening capacity-building and digital resilience in the Global South became an emerging priority.

8. Rapid Expansion of the Cybercrime Economy
   APT41's monetization tactics, such as stealing virtual currency, credit card data, and in-game assets, highlighted the growing overlap between state operations and cybercrime markets. This raised alarms about how quickly the cybercrime economy was evolving, and how state actors could launder or monetize cyber intrusions in ways that are difficult to trace. It pushed law enforcement and financial institutions to rethink their models for digital forensics, crypto tracking, and cross-border crime prevention.

Recommendations from the Executive Board

Executive Board Recommendations for Delegates

The Executive Board extends a warm welcome to all delegates participating in this committee session. As we approach an intellectually rigorous and diplomatically demanding agenda, it is imperative that delegates align themselves with the expectations and standards of this simulation. This committee reflects a model of the real-world United Nations Security Council, and accordingly, the decorum, preparedness, and conduct expected from each delegate must mirror the seriousness of such a setting.

1. Research & Preparation:
Thorough research is the foundation of meaningful contribution. Delegates are strongly advised to engage in in-depth study of the agenda, their country's stance, and their assigned portfolio. Particular attention must be paid to previous international efforts concerning cybercrime, such as the Budapest Convention (2001), the UN GGE reports (notably 2010, 2013, 2015), UNGA Resolution 74/247 (2019) and the Shanghai Cooperation Organization's frameworks, among others till 2020. Understanding your country's engagement with these instruments is essential to drafting practical and representative solutions. This background guide should not be your main source of research, nor can it be quoted in your speeches or paperwork. This should just be your starting point to know what to research and know what points to cover in committee.

2. Formatting & Structure:
Professional formatting reflects the seriousness of your directives and working papers. Submissions must follow standard diplomatic formatting with clarity, logical flow, and proper labeling. Disorganized or improperly formatted documentation will not be entertained or evaluated favourably.

3. Responsibility of Actions:
Every statement made and every directive proposed holds weight. Delegates must understand that their actions—be it a strong resolution, an aggressive stance, or an attempted compromise—will have in-committee consequences. These may be beneficial, detrimental, or neutral, but they will always be evaluated.

4. Realistic Simulation:
This committee is a simulation of a real United Nations session. Thus, personal opinions must be kept separate from official country policy, and delegates must consistently reflect their country's international positions. The goal is to maintain authenticity while pushing for viable and impactful solutions.

5. Quality over Quantity – Directives:
We strongly encourage **comprehensive directives** that contain multiple **sub-directives**, each addressing different aspects of the crisis or issue. Fragmented, isolated directives will be seen as less effective and less strategic in nature. Delegates must approach problem-solving with depth and coordination.

6. Lobbying & Diplomacy:
Lobbying is a vital aspect of this committee and will be **graded**. Delegates must take initiative in forming blocs, co-sponsoring directives, negotiating compromises, and building consensus. Active and ethical diplomacy is a key measure of performance.

7. Discipline & Conduct:
Professionalism and decorum will be strictly maintained. Delegates are expected to be punctual, attentive, and respectful at all times. Any breach in discipline—including disruptions, disinterest, or disregard for rules—will result in a **deduction of marks**.

In conclusion, this committee is designed to challenge your research abilities, critical thinking, and diplomatic acumen. The Executive Board looks forward to a productive, engaging, and high-standard session. Let every action be deliberate, every word well-chosen, and every decision made with the awareness of its global consequences.

Further Reading

APT41 and Recent Activity. 2022, www.hhs.gov/sites/default/files/apt41-recent-activity.pdf.

capsnetdroff. "Decoding Chinese Hacking Syndicate – APT 41." *CAPS India*, 4 Aug. 2022, capsindia.org/decoding-chinese-hacking-syndicate-apt-41/.

CAUTION. www.fbi.gov/wanted/cyber/apt-41-group/apt-41-group-cyber-wanted-web.pdf. Accessed 27 June 2025.

"Connect the Dots on State-Sponsored Cyber Incidents - APT 41." *Council on Foreign Relations*, www.cfr.org/cyber-operations/apt-41.

FBI. "APT 41 GROUP." *Federal Bureau of Investigation*, www.fbi.gov/wanted/cyber/apt-41-group.

News, The Hacker. "Chinese APT41 Exploits Google Calendar for Malware Command-And-Control Operations." *The Hacker News*, 29 May 2025, thehackernews.com/2025/05/chinese-apt41-exploits-google-calendar.html.

"Seven International Cyber Defendants, Including 'Apt41' Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally." *Justice.gov*, 16 Sept. 2020, www.justice.gov/archives/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

The Justice Department. "7 Cyber Defendants, Including 'Apt41' Actors, Charged in Connection W/ Computer Intrusion Campaigns." *YouTube*, 16 Sept. 2020, www.youtube.com/watch?v=tY0VvmdW8J0. Accessed 27 June 2025.