Cyberdefending Taiwan: Lessons from Ukraine

Conference Report

Chris Jay Hoofnagle

November 15, 2023

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Introduction

Authoritarianism is rising worldwide. Rule of law is declining in most countries. The internet makes possible many rule-*by*-law intrusions upon civil liberties.

The ongoing tension between Taiwan and China is among the most consequential struggles for freedom in the world. Taiwan is a thriving, multi-party democracy, assessed by Freedom House as having freedom in political processes, in the judiciary, and in personal autonomy. If Taiwan were to be subjugated by the Chinese Communist Party (CCP), a nation "profoundly oppressive and…the world's worst abuser of internet freedom,"[1] it would be a cataclysmic loss of freedom for the Taiwanese, would upset regional efforts to center human rights, and continue the trend of world authoritarianism.

It is entirely within Taiwan's sovereign choice to deepen its civil defense. To better understand Taiwan's cyber-domain options, the Center for Long Term Cybersecurity (CLTC) convened a one-day symposium, *Cyberdefending Taiwan: Lessons from Ukraine*, at the University of California, Berkeley, on September 29, 2023. The event focused on the cybersecurity, not the kinetic, aspects of the conflict between Taiwan and China.[2] As the title suggests, panelists leveraged lessons from Russia's February 2022 invasion of Ukraine to inform Taiwan's posture. This short report summarizes the main takeaways from the event.[3]

[1] See Freedom House, *Freedom in the World 2023*.

[2] For an excellent overview of the conflict and its kinetic elements, see Kori Schake and Allison Schwartz. *Defending Taiwan: Essays on Deterrence, Alliances, and War*. AEI: American Enterprise Institute for Public Policy Research, 2023. URL: `https://www.defendingtaiwan.com/`

[3] Thank you to Rachel Wesen, Matthew Nagamine, Shanti Corrigan, Chuck Kapelke, and Ann Cleaveland for their support in making this event possible.

1 Lessons from Ukraine

Looking back at the February 2022 Russian invasion of Ukraine and previous Russian cyberattacks, the symposium's first panel surfaced several lessons that might be applied to Taiwan. The panel was moderated by Andrew Reddie, Founder, Berkeley Risk and Security Lab; Associate Research Professor, UC Berkeley Goldman School of Public Policy.

Key Takeaways

- The International Criminal Court (ICC) can justify its investigation into cyber war crimes on a preexisting armed conflict in Ukraine, a status that is not present in Taiwan. Ukraine also benefited from a political landscape where governments and companies were willing to attribute Russian attacks—an inclination that is not mirrored for Taiwan.
- Russia's attack has given the U.S. and its allies, so-called like-minded states, a bigger role in driving international governance norms.
- Like Russia, China has developed sophisticated capabilities in space and anti-satellite techniques.
- Ukraine relied upon private satellite service to great effect; Taiwan must also develop greater satellite communications capacity and ensure that it is resilient to economic and political influence levied against the satellite provider.
- The FBI provided support in sharing classified intelligence, in coordinating a whole-of-government response to Russian attacks, and critically, in helping Ukraine liaise with US-based social media surrounding disinformation. Taiwan could benefit from building similar relationships now.

Human rights law as a remedy for Russia's aggression

Lindsay Freeman, Technology, Law, and Policy Director, Human Rights Center, UC Berkeley School of Law, focused on whether Russian cyber attacks on critical infrastructure in Ukraine could constitute war crimes under the Rome Statute, which governs the International Criminal Court (ICC). Freeman's method is comparative and informed by the Chinese strategic approach as expressed in Unrestricted Warfare[1] and the so-called Gerasimov Doctrine.[2] Freeman's Human Rights Center has filed two "Article 15" filings with the ICC to substantiate Russia's aggression.

Drawing upon her years-long study of Russian cyber aggression, Freeman offered four observations comparing the situations in Russia and China. Most importantly, Russia has delivered highly consequential cyberattacks against Ukraine, and the targets of these attacks are counter-value (i.e., targeting civilian assets). For instance, Russian attacks on Ukraine's power grid, which began as early as winter 2015, affected civilians located far from the battlespace of Crimea. Civilians suffered from these attacks, and Russia impaired the functionality of civilian critical infrastructure. Turning to Taiwan, Freeman argued that China has targeted the nation with a huge volume of lower-intensity attacks. To date, Taiwan has experienced no single incident that has compared in magnitude to the Russian attacks.

Second, the Russian-Ukraine contest is formally an armed conflict. The conflict's status allows the ICC to directly examine Russia's activity. Without an armed conflict, the ICC would have to examine whether Russian cyberattacks were "armed attacks." This factor, along with the lower-intensity nature of China's attacks, contributes to a different legal landscape for Taiwan. There is no formal armed conflict between China and Taiwan. Together these factors create a legal hurdle for Taiwan, because it cannot point to cyberattacks that have created casualties or damage typical of a kinetic attack.

A third point relates to attribution. In the wake of cyberattacks on Ukraine, a global consensus emerged pointing to Russia, and specifically an attack group known as "Sandworm," as being responsible. Turning to Taiwan, a greater effort is needed to mobilize formal attribution of attacks against the nation.

Finally, the ICC does not have universal jurisdiction and the strongest cyber and

[1] Qiao Liang and Wang Xiangsui. *Unrestricted warfare*. PLA Literature and Arts Publishing House, 1999. url: https://www.c4i.org/unrestricted.pdf

[2] Valery Gerasimov. "The value of science in prediction". In: *Military-Industrial Kurier* 27 (2013), Charles K Bartles. "Getting gerasimov right". In: *Military Review* 96.1 (2016), pp. 30–38. url: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf

military powers have tended to eschew the court. Ukraine, however, consented to ICC jurisdiction in 2014, giving the ICC power to investigate and prosecute Vladimir Putin. Indeed, the ICC has formally launched an investigation into war crimes and issued an arrest warrant for Vladimir Putin.[3] Neither China nor Taiwan is a state party to the Rome Statute, the treaty that established the ICC.

The Russian invasion's effects on governance

Elaine Korzak, Research Fellow, UC Berkeley Center for Long-Term Cybersecurity, explained how Russian aggression has altered international governance and norms processes surrounding cyber attacks. To set the stage, Korzak explained the different concepts of cybersecurity among states. Authoritarian nations, she explained, make *information* the focus of cybersecurity—for example, by seeking treaties to regulate information flows to their populations, and to vest sovereign control over this information. By comparison, the US, EU, and other like-minded nations focus cybersecurity on the confidentiality, integrity, and availability of *computing systems*, rather than information itself.

Aside from different assumptions about the purpose of cybersecurity, Russia and China oppose the application of international humanitarian law to cyberspace, reasoning that the application would in effect militarize it. Here, too, the West is diametrically opposed: efforts such as the Tallinn Manual demonstrate the commitment to translate human rights norms and international humanitarian law into uses of technology for military purposes.[4]

Korzak explained that the Ukrainian attacks, at least in the short term, have reversed the roles of Russia and the West. Traditionally, the Russians have driven the process of promoting an information-control-paradigm treaty. The war has given the US and like-minded governments an advantage in driving governance norms.

Going forward, Taiwan must leverage the sense of urgency that Ukraine successfully actuated to rally allies and international support. Moderator Andrew Reddie connected this sense of urgency to changing norms in Silicon Valley: back in 2018, some Google employees loudly objected to the company participating in the Department of Defense's computer vision efforts, known as Project Maven. In recent years, Google and other firms seem to have changed course and now

[3] https://www.icc-cpi.int/situations/ukraine

[4] See also Bart Hogeveen. "The UN norms of responsible state behaviour in cyberspace". In: (2022)

regularly pursue defense projects, such as the Joint Warfighting Cloud Capability (JWCC) program.

Ukraine's cybersecurity context

Aleksandr Kobzanets, Special Agent, Federal Bureau of Investigation, was deployed in Kiev during the Russian invasion as a legal attaché. FBI operates scores of such offices around the world in a mission that promotes both law enforcement and diplomacy.

Prior to the invasion, cyberattacks routinely came to Kobzanets' attention in his law enforcement role. These were ordinary cybercrimes and other malicious activity that had a nexus to Ukraine in the form of infrastructure, bulletproof hosting, and even suspects hiding in the country. This initial observation—that Ukraine was entangled in cybercrime—may have helped the nation in its defense against Russia. Ukrainians have developed a great deal of cyberattack expertise.

But after the invasion, Kobzanets' activity was more diplomatic in nature. The FBI bolstered Ukraine's defense in several ways: First, the FBI liberalized its classified information sharing policy, passing on more information, more quickly to partners in Ukraine. Second, the FBI helped in whole-of-government coordination in intelligence. This challenging task involves identifying who in the Ukrainian government is responsible for which form of response, all in the midst of a dangerous and dynamic situation. Third, the FBI assisted Ukraine by providing cyber capabilities. Fourth, the FBI traced Russian cyber activity on US-based social media providers and helped the country interact with those US providers, particularly surrounding disinformation efforts.

Perhaps the international community initially underestimated Russia's cyber activity. One early attack appeared to only cause web defacement, but upon inspection was an industrial wiper, among the most consequential forms of attack.

Kobzanets shared several insightful anecdotes, including the experience of evacuating by car convoy and the destruction of the American embassy to avoid Russian acquisition of US secrets. Particularly revealing was a January 2022 cyberattack by Russia; in retrospect, this attack may have been a form of practice, as similar techniques were used a month later with the invasion.

Turning to Taiwan, Kobzanets recommended that any nation facing the prospect of aggression should start creating relationships with agencies such as the FBI, and with private-sector media providers, well before actual aggression. The "practice" attack by Russia in January 2022 suggests that careful study of China—to observe its preparation, and even its mistakes—may help Taiwan envision and prepare for China's operations and tactics.

Space as a central theme

Gil Baram, Postdoctoral Scholar, UC Berkeley Center for Long-Term Cybersecurity, warned that aggression against Taiwan occurs against the backdrop of increasing Chinese capability and ambition in space.[5]

Baram focused on Russia's attacks on Viasat's KA-SAT network terminals, which caused a key, consequential outage. How Russia carried out the attacks is important—Baram explained that satellite attacks could focus on the space vehicle itself, the communications link to the ground, and/or user hardware that manages access to the satellite. There are many options for such attacks, ranging from kinetic missiles to lasers and other jamming techniques, but each of these choices has major downsides, from creating dangerous space debris to only causing a temporary communications blackout. A poorly tailored attack could have effects far outside Ukraine, possibly triggering retorsion from a NATO country.

Russia chose to use cyberattacks to destroy Ukrainian access terminals, rendering them inoperable and not repairable. The effects were relatively localized.

Ukraine quickly pivoted to private-sector satellite capacity provided by Elon Musk's StarLink. StarLink has natural resilience against attack because the network is a mega-constellation of over 4,000 vehicles. Like a mesh network, an attack on any one vehicle is inconsequential, as traffic is passed to other satellites.

While technically resilient, SpaceX the company is subject to political and economic pressure, and the esoteric whims of the company's CEO. And as the constellation is used for military purposes, it could become a legitimate target of attack under the Law of Armed Conflict.

Turning to Taiwan, the nation has learned several lessons from the Ukraine attack. In particular, the nation is planning its own satellite communication system. The puzzle Taiwan faces is how to leverage the resourcefulness of the private sector while avoiding its political and economic soft spots. Baram also suggested that regional and other allies would be critical for Taiwan's cyber defense.

[5] See Gil Baram. "Securing Taiwan's Satellite Infrastructure Against China's Reach". In: *LawFare* (2023)

2 Taiwan: Cables, Constellations, Chips

The second session in the symposium transitioned to the Taiwan security context, both to better understand Taiwan's posture with China as a competitor and to differentiate Taiwan's situation from that of Ukraine. Panelists discussed the characteristics of Taiwan's internet infrastructure and how it might resist physical or logical cyberattack, the larger technology competition strategy between the U.S. and China, and how China's prowess in outer space affects its cyber posture with regard to Taiwan. The session was moderated by Professor Vinod (Vinnie) Aggarwal, Director, Berkeley Asia Pacific Economic Cooperation Study Center, and Professor, UC Berkeley Travers Department of Political Science.

Key Takeaways

- Tensions in the underlying US–China relationship are creating "strategic weather" for Taiwan.
- Differences in China's internet infrastructure have strategic implications: China can simply disconnect many of Taiwan's cables, and China's internet infrastructure may be more resilient against attack.
- Innovations in the private-sector satellite industry provide some promising options for both communications and geospatial intelligence gathering, but even the newest-generation satellites lack the capacity to fully replace cables.

Cables

Nick Merrill, Director, Daylight Security Research Lab, UC Berkeley Center for Long-Term Cybersecurity, explained that today's internet primarily relies upon fiber optic cables. This means that the internet is a material thing—and much of the internet's infrastructure exists within (and thus a significant amount of traffic relies upon) the United States. For Taiwan, as an island nation, cables are particularly important. According to TeleGeography, Taiwan has 14 submarine internet cables, with the 15th (Apricot) scheduled for operation in 2026.[1]

Taiwan's plight is that China can disconnect these cables without kinetic action. Nine of Taiwan's cables can be disconnected logically by China.[2] Recognizing this, the U.S. has attempted to bolster Taiwan's internet resilience. The U.S. government opposed plans by Google and Facebook to connect a new cable between the U.S. and Hong Kong, resulting in the companies making a new pitch to connect the US, Taiwan, and the Philippines. The companies are also encouraged to interconnect with Indonesia, Thailand, Singapore, and Vietnam, but have promised not to connect with Hong Kong.

Unlike the targeted attacks on Viasat terminals discussed by Gil Baram, disconnecting Taiwan's cables would create extreme internet congestion regionally and perhaps worldwide. The reason, Merrill explained, is that the terminated connections require the Border Gateway Protocol (BGP) to recalculate routes. (This is the so-called "routing around censorship" property of the Internet Protocol.) This process is less resilient than idealized, and could lead to an extended period of congestion worldwide. Furthermore, the nine cables connect other regional nations, creating additional opportunities for increased congestion.

Yet another risk comes from selective filtering of communications through the cables that China controls. For instance, China might selectively allow the passage of communications it prefers, while blocking others. The good news is that newer internet protocols, such as TLS 1.3, obscure more communications metadata, making filtering more difficult.

Ukraine relied upon StarLink for internet access after the attacks on Viasat and the nation's terrestrial communications. Turning to Taiwan, there is no hope that satellites can replace the bandwidth provided by fiber-optic cable. Yet Taiwan is building domestic satellite communications capabilities to at least preserve government access during a conflict. Merrill floated two other approaches: point-to-point microwave networks, supported by nearby allies; and local municipal mesh networks. Mesh networks can be resilient against attacks, in part because mesh devices can be hidden (e.g., on rooftops).

Merrill also explained that China's internet design may give it an attacker advantage. The reason relates to the proliferation of content delivery networks (CDNs) in the West, a centralizing technology that is not as popular in China. Merrill's

[1] See https://www.submarinecablemap.com/

[2] Merrill provides an in-depth analysis here https://www.else.how/p/taiwan-and-the-internet-during-world, Perma.cc link: https://perma.cc/7LJR-XGVG

research has shown that disruption at even minor CDNs can cause substantial outages.[3]

Constellations

Picking up on the themes introduced by Gil Baram, Benjamin Bahney, Senior Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory (LLNL), explained the dynamics of satellite communication and how advances in technology have changed the landscape. The newest generation of private satellite communications companies such as StarLink (and emerging competitors such as Amazon Kuiper Systems and OneWeb) use low Earth orbit (LEO), and thus have several advantages over older geosynchronous equatorial orbit (GEO) vehicles. LEO satellites, because they are closer to the communicating parties, have much lower latency and much higher bandwidth than GEO constellations.

Just as important is access to space. The innovation of reusable launch vehicles and the increased frequency of launches creates more incentives and opportunities for firms to develop and deploy new technologies. Access to space is becoming less expensive, creating a new space race.

China has significant anti-satellite capabilities, for instance mobile jammers that can deny satellite communications, particularly GEO-based communications. "Dazzlers" can flood optical sensors, thus blocking intelligence, surveillance, and reconnaissance satellite (ISR) capacity from private companies such as Maxar, Planet, and BlackSky. China has kinetic kill capability against satellites, and of course cyberattack capabilities.[4] LEO satellites have more resilience against jamming and dazzling because they move so quickly across the sky, but face the same risk from kinetic and cyberattacks.

Looking forward, Taiwan can develop public-private partnerships with satellite providers for both LEO communications and ISR.

Chips

Graham Webster, Research Scholar, DigiChina Project, Program on Geopolitics, Technology, and Governance at Stanford University, began by emphasizing the

[3] Nick Merrill and Tejas N. Narechania. "Inside the Internet". In: *Duke Law Journal Online* 73 (2023)

[4] Defense Intelligence Agency. *Challenges to Security in Space*. Tech. rep. 2022. url: `https://perma.cc/5HKU-VM6Z`

strategic and existential relationship between the US and China: the nations are bound by worldwide challenges such as climate change, decarbonization, and the maintenance of peace, challenges that cannot be solved without collaboration. At the same time, espionage and sabotage risks are heightened from the nations' technological interdependence through the internet, and through the supply chain. Taiwan is on the front of the "strategic weather" created by these tensions.

The CHIPS and Science Act of 2022, Webster explained, represented a "turning point" in US strategy, an attempt to grow domestic production of chips, and therefore reduce reliance on Taiwan, while also hampering China's importation of chips and efforts to build their own fabrication labs.

3 Defending Taiwan: Priorities and Opportunities

The third panel in the symposium analyzed what the public and private sector should be doing now and over the next two to three years to secure Taiwan. Professor Janet Napolitano, Director, Center for Security in Politics, and Professor, UC Berkeley Goldman School of Public Policy, moderated the session.

Key Takeaways

- Taiwan is expanding compulsory military service and creating new institutions and laws in order to defend against China.
- Taiwan faces challenges in creating resilience for its energy production and its positioning, navigation, and timing infrastructure.
- The Defense Innovation Unit's methods for deciding what to procure offer a model for quick adoption of defense technologies useful to Ukraine and Taiwan.

The strategic context

Professor Hung-dah Su, Dean, College of Social Sciences; Professor, Department of Political Science, National Taiwan University, explained the strategic landscape of the "Asian Mediterranean:"

- Taiwan is rethinking its energy diversity, including by reconsidering a commitment to denuclearization made prior to the escalation of tensions with China. Energy is a critical factor, and Taiwan has a distressing dependence on non-renewable sources, and a limited, vulnerable strategic reserve.

- Taiwan's foreign trade is dominated by China, but is shifting to regional allies and the U.S.
- Taiwan is hardening its submarine cable landing points and constructing new cables without a mainland China landing.
- Taiwan is creating its own LEO satellite communications system, yet this will only provide a small percentage of needed internet capacity.

Taiwan is the target of overwhelming disinformation attacks, with a 2018 Digital Society Report finding that the nation is targeted "extremely often. Foreign governments disseminate false information on all key political issues." Some of this disinformation is consequential; one campaign resulted in the 2018 suicide of a Taiwanese official shamed by PRC-generated disinformation. The Chinese People's Liberation Army (PLA) has units devoted to cyber aggression against Taiwan, and support is provided by the "little pinks," internet-savvy nationalists.

In response to these campaigns, Taiwan has enacted new laws proscribing disinformation and created new institutions to fight it. NTU itself has created a new research center devoted to social resilience. Taiwan has mirror institutions to many cybersecurity organizations in the U.S., such as the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) and the recently created Ministry of Digital Affairs (MODA).

Taiwanese institutions are engaged in standard cybersecurity resilience activities, but apparently have not pursued large-scale exercises like the U.S. Government's "Cyber Storm." Su suggested that large-scale activities might undermine trust in government.

On the military front, Taiwan has increased conscription time from four months to 12, which is typically an unpopular move among citizenry, but in Taiwan's case was met with approval. Su reported that women are clamoring to be included in compulsory military service.

An operational perspective

Tim Mather, Partner and vCISO, Fortium Partners, provided an operational diagnosis of Taiwan's predicament from the perspective of a private-sector chief information security officer (CISO). Mather focused on resilience on the civil side of the defense of Taiwan:

- Data backups, cryptographic keys, and infrastructure-as-code tools used to re-instantiate cloud infrastructure should be moved off Taiwan, according to Mather.

- Consistent with Nick Merrill's discussion in the first panel, Mather recommended development of communications compatible with local mesh networks.
- Precise positioning, navigation, and timing (PNT) are important to both computing and defensive efforts. China and Russia frequently block or degrade global positioning systems. Perhaps Taiwan can rely on satellites such as StarLink or OneWeb for PNT. Taiwan has only a single atomic clock for precision timing.
- Taiwan probably faces a weaker posture than Ukraine in reliance on StarLink for communications and PNT. Elon Musk has deep economic dependency on China and may bend the knee lower to Xi than Putin.

Aligning public and private sectors

Ritwik Gupta, Deputy Technical Director for Autonomy, Defense Innovation Unit (DIU), explained the DIU's approach to creating public-private partnerships that could benefit Ukraine and Taiwan.

DIU adopts a "fast follower" approach, meaning that it quickly adopts and adapts innovations that the private sector creates. This allows the Department of Defense to leverage a much larger pool of investment across sectors. The difference is subtle and important. Funding entirely new innovations suffers from monopsony-oligopoly dynamics. With the government as the sole buyer, contracts tend to be won by a small number of existing defense primes. DIU's idea is that by only funding existing offerings, as a buyer the government is operating in a more competitive marketplace. Conversely, the process could contribute to resilience, as the government is not the sole customer of these companies. Another benefit is that with the government as a customer, any product improvements made at the request of the government could seep into commercial versions of the same technology.

Procurement rules weigh heavily on innovation. As procurement rules accrete, companies that win contracts might be those that are good at procurement processes, rather than the entities with the most needed innovations. To address this, DIU has special procurement authority (similar to NASA and DARPA) with surprisingly fast resolution. DIU posts a short problem statement that vendors with an existing product can respond to with a short slide deck or memo. The special protocol has enabled some purchases to take less than two months.

Turning to technologies, a class of satellite geospatial intelligence applications funded by DIU are relevant to both Ukraine and Taiwan. These technologies sense ships using computer vision and match their locations to other sources. For instance, Gupta described “dark vessel” detection: the project involves comparing sightings of ships using synthetic aperture radar by satellite and comparing it against the “Automatic Identification System,” a tracking system all ships are required to broadcast. Such systems can illuminate vessels that are trying to evade detection in order to engage in illegal fishing or perhaps *sub rosa* military or intelligence purposes.

Unmanned Aerial Vehicles (UAVs, commonly referred to as “drones”) are another technology relevant to both Ukraine and Taiwan that present significant security risks. Adversaries can use both cyber and electronic warfare techniques to defend against commercial drones. Gupta explained that the problem is worse with “swarms” of UAVs because groups of the devices may be vulnerable to attacks on single vehicles. DIU has helped the military reduce its dependence on commercially available UAVs in favor of more secure implementations.

4 The Chinese Cyber Threat and What Taiwan Can Do

Raymond Kuo is the inaugural Director of the Taiwan Policy Initiative and a Senior Political Scientist at the RAND Corporation. He is an expert on international security, international order, and East Asia. Raymond's first book – *Following the Leader: International Order, Alliance Strategies, and Emulation* – explains how military alliance strategies generate international order. His second book – *Contests of Initiative: Confronting China's Gray Zone Strategy* – recommends three courses of action for the U.S. to defeat and deter Chinese coercion in the East and South China Seas. Kuo gave the lunchtime keynote at the conference.

Key Takeaways

- China is Taiwan's main cyber adversary. The majority of successful attacks against Taiwan are attributed to China.
- China's perception of cyber is that it presents a potential catastrophic threat, but also that China lags behind the U.S. (and others) in cyber, space, nuclear, joint domain command and control, and other military capabilities.
- Subversion—not sabotage or espionage—is the key cyber threat to Taiwan. Yet the Taiwanese have many growing sources of resilience against subversion.
- The U.S. could support Taiwan and the region by making stronger assurances that it will defend Taiwan.

Chinese strategic thinking about cyber

The publicly available summations of Chinese cyber doctrine reflect well-known misconceptions about cybersecurity.[1] Kuo observed that the Chinese see cyber as offense-dominant, as offering anonymity, as inexpensive, as providing a mechanism to attack high-value critical infrastructures, and as creating catastrophic consequences—loss of government control, collapse of national security, etc. However, the reality, Kuo observes, is both more nuanced and deeply explored by security studies scholars.[2] For instance, as of this writing, there have been no examples of mass killing from cyberattacks. Consequential destructive cyberattacks require exquisite design and careful efforts. As evidence, consider the Stuxnet attack, which required extensive simulation, investment, and design. When most government decision-makers seek to effect destruction, they tend to use bombs instead of cyber. Bombs are more reliable than cyberattacks, belying cyber's reputation as a perfect weapon.

China's goal is to upset the internet as a domain, converting it from a multistakeholder asset (one governed by complex compromises among governments, companies, and NGOs) into a sovereign information control domain (where nations can impose censorship or reshape perceptions with information inside their borders). Calling back to Korzak's presentation, Kuo's point is that China and Russia see Western assumptions about security (the view that security should concern itself with technical issues) as promoting values of free speech and democratic participation. China and Russia, as security-as-information-control advocates, wish to convert security into a tool that empowers their censorship. If China and Russia are successful, the internet would not spread free speech, but rather systematic, pro-authoritarian information control. As part of this process, China wants to bar many of the most popular application-level services from the country, because most of these are American.

China's ambition to influence others' minds is broader than Western nations may understand. China believes that anyone with Chinese decent—even U.S.-born people—is within scope of the nation's propaganda efforts.

[1] "To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misconceptions and misunderstandings." Richards J Heuer. *Psychology of intelligence analysis*. Center for the Study of Intelligence, 1999. url: https://perma.cc/N534-CYVP

[2] The classic work in this genre is Thomas Rid. "Cyber War Will Not Take Place". In: *Journal of Strategic Studies* 35.1 (2012), pp. 5–32

Subversion and resilience

Subversion—attacks on people's minds, and on their trust in government and institutions—is the cyber risk most threatening to Taiwan, according to Kuo.

For subversion to work, an attacker has to understand how to create compelling memes. This requires cultural context and knowledge—a problem for Taiwan because China has deep understanding of Taiwan.[3] China possesses a wide variety of institutional tools and efforts to influence people in Taiwan. Taken together, Freedom House assesses Chinese media influence efforts in Taiwan as "very high."

Yet Taiwan also has strong aspects of resilience against subversion, according to Kuo, and according to Freedom House, which rates the local resilience as "very high." One compelling data point can be seen in the declining number of Taiwanese who identify as Chinese, as well as rising nationalism reflected in the growing number of people reporting their identity as Taiwanese only. Meanwhile, as a result of witnessing the erosion of freedom in Hong Kong the Taiwanese increasingly do not believe the messages emerging from Chinese apparatchiks. Finally, Taiwan has a number of government institutions tasked with resisting disinformation.

A strategy more about America than Taiwan

Kuo warned that the U.S. may anticipate worst-case-scenario events, but what is more likely is a collection of more subtle events that erode the will of the U.S. and the Taiwanese to resist China.

When the U.S. wavers on its international security commitments, it creates region-wide uncertainty and risk aversion. The slightest wavering can create uncertainty; for instance, some detractors criticize the U.S. for not directly fighting Russia after the invasion of Ukraine, arguing that the mere provision of weapons (rather than troops) demonstrates a lack of true commitment. This suggests that some Taiwanese want the U.S. to make a commitment to putting troops on the ground in the case of growing Chinese hostilities.

Kuo argues that if regional actors are unsure of America's intent, the effect will be to:

[3] Kuo points to the Doublethink Lab as a good source for evidence of Chinese intrusion into Taiwanese affairs https://doublethinklab.org/

- Reduce Taiwanese social cohesion;
- Increase aversion to risk;
- Reduce alignment between Taiwan and the U.S.;
- Make Taiwan's defense weaker; and
- Complexify international coordination.

Growing regional insecurity may present Taiwan with more active regional allies. For instance, South Korea, which has mainly focused on threats from North Korea, is now more involved in regional security matters. Other allies stretch from Australia to India.

Kuo suggested that the expressed policy of "strategic ambiguity" may be weakening Taiwan's resolve. A stronger statement of commitment would create greater regional cybersecurity coordination, enhance communications, and support exchange between government and civil society.

5 Transnational Repression

Jeffrey Fields, Assistant Special Agent in Charge of the FBI's Counterintelligence Branch in San Francisco, ended the symposium with a keynote on "The Challenge of Transnational Repression" presented together with an FBI colleague.

Key Takeaways

- Transnational repression (TR) occurs when foreign governments or their agents intimidate U.S. persons into silence. To be clear, foreign students are U.S. persons who enjoy the full bundle of American free speech and privacy rights.
- TR is a problem on the University of California, Berkeley campus—and other large campuses.
- TR threats come from China, but also Iran, Saudi Arabia, Turkey, and even India.
- Faculty should not assume that students who mention pressures of being a foreign student are reporting on other students.
- TR can be reported to the FBI; students who are uncomfortable with reporting still benefit from faculty members who lend a sympathetic ear.

In Nov. 2022, anonymous Chinese students wrote in the Daily Cal, UC Berkeley's newspaper, that, "while studying at UC Berkeley, certain instances show that if we openly express disagreement, our parents and relatives in China could be targeted by police. We may even experience similar treatment when we go back to our home country in the future. Consequently, we know many of the Chinese students overseas, including us, generally remain apolitical or are afraid of sharing their own thoughts."[1] The FBI refers to this activity as "transnational repres-

[1] Anonymous Chinese Students. "The Poster Movement: A lonely protest in Beijing echoed by politically awakening Chinese students overseas". In: *Daily Cal* (Nov. 2022). url: https://dailycal.org/2022/11/17/the-poster-movement-a-lonely-protest-in-beijing-echoed-by-politically-awakening-chinese-students-overseas

sion" (TR), which it defines as "foreign government transgression of national borders through physical and digital means to intimidate, silence, coerce, or harm US-based individuals—in violation of international norms, U.S. laws, and individual rights and freedoms." TR is not a new problem, but has expanded in scale and scope in a world connected by the internet.

The TR problem nationally

People come from all over the world to U.S. educational institutions to explore new ideas; this is part of America's soft power to promote liberalism and tolerance. TR erodes Western soft power influence, imperiling students even when they are in America and have an opportunity to explore different ideas, different politics, and even non-conforming gender roles. Fields explained that TR hits at the center of American civil liberties by chilling free speech.

Fields' team explained that foreign governments and their agents use TR to compel compliance with some demand (even for purposes such as making a court appearance), to silence opposition, and even to recruit U.S.-based diaspora members. TR may be pursued by foreign government officials directly (this is frequently done through internet services, rather than in person), or through proxies, including private investigators and sometimes family members, which means the suasion may take place in person.

Fields' team used three examples of criminal prosecutions brought to protect U.S. persons (Masih Alinejad, Iran; Xiong Yan, China; and Mo Peifen, China) from plots to silence and/or abduct them. TR is increasing in frequency and intensity. Traditionally, TR focused on foreign U.S. persons, but governments and affiliated movements now target U.S.-born individuals.

TR from China tends to follow student activities based on one of the "five poisons:" discussions of freedom for Taiwan, Falun Gong, Uyghurs, Tibetan independence, and pro-democracy efforts generally. TR tactics include:

- Extortion or blackmail;
- Cyber attacks, malware, hacking, and surveillance;
- Doxxing (posting the personal information of a dissident);
- Harassment, threats, and intimidation;
- Rumor spreading surrounding sexual activity;
- Disinformation campaigns;
- Threats to family members or friends of imprisonment;

- Harassment, when the target is traveling in a third country with weak civil liberties protections or where the third country has an extradition treaty with the coercing country; and
- Forced repatriation through threats or revocation of passports.

TR at UC Berkeley

The FBI team was reluctant to discuss specific examples at the University of California, Berkeley, but claimed that most large U.S. campuses have TR problems. Many TR incidents are associated with branches of the "Chinese Students and Scholars Association" (CSSA), organizations created and supported by the PRC that pressure students to join and participate in PRC political activities.

The author of this report received several examples of TR that were volunteered by other UC Berkeley faculty members. These examples are perturbed to prevent attribution:

- ...some of our LGBT Studies students from an array of countries are in a similar situation of potential danger if they are recorded in classes ...
- I have encountered this issue extensively before! One student even refused to do a project visualizing ambiguity, saying that "the party" pursues harmony only.
- We had a HUGE issue when we hosted an event ...on the Uighur crisis (students interrupting the speakers, recording the audience even though we'd banned cell phones from being brought into the room, etc.).
- A faculty member who used to host students with China wrote ...with each group, I would know there was an informer in a bunch...These days I believe they are incentivized to report on one another even more than in the past. It is a sad state of affairs, but it is one that has long existed.

What to do about TR?

Fields encouraged students to speak with a trusted person about TR. Students obviously do not need to discuss it directly with the FBI. The team emphasized that students who raise concerns about "pressures" should not lead to the conclusion that the student is reporting on other students. Instead, faculty ought to listen sympathetically and attempt to diagnose the kind of pressure the student is discussing.

Fields' team points to an FBI website, which provides information defining TR[2] and how to report incidents of TR to the FBI.[3].

[2] FBI. *Transnational Repression*. url: https://www.fbi.gov/investigate/counterintelligence/transnational-repression

[3] FBI. *Threat Intimidation Guide*. url: https://www.fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view. We have posted Perma.cc versions of these documents at https://perma.cc/G73K-FNMH and https://perma.cc/FY76-6VKK

Participant Bios

Vinod (Vinnie) Aggarwal is Distinguished Professor and holds the Alann P. Bedford Endowed Chair in Asian Studies, Travers Department of Political Science; Affiliated Professor at the Haas School of Business; Director of the Berkeley Asia Pacific Economic Cooperation Study Center (BASC) at UC Berkeley; and Fellow, Public Law and Policy Program, Berkeley Law. His current research examines economic statecraft in high technology sectors in the context of great power competition.

Benjamin Bahney is the Program Leader for Space at Lawrence Livermore National Laboratory and a Senior Fellow at the Center for Global Security Research (CGSR). At CGSR, Ben studies strategic competition in the 21st century, with a particular focus in the areas of space, cyber, and advanced science and technology. His research interests include how these new areas of competition affect strategic stability, deterrence, and escalation management.

Dr. Gil Baram is a cyber strategy and policy expert with more than 15 years of experience leading innovative research, lecturing, and consulting senior business leaders and government officials. At present, she is a Postdoctoral Scholar at the UC Berkeley Center for Long-Term Cybersecurity. Her research focuses on governmental decision-making during cyberattacks and strategic attribution-related policy. She works at the intersection of cyber and international security, examining under what circumstances governments choose public disclosure of attacks or secrecy, the role of intelligence agencies in cyberattacks, cyber threats to space systems, and more.

Jeff Fields currently serves as the Assistant Special Agent in Charge of the FBI's Counterintelligence Branch in San Francisco. For more than 16 years, Jeff has conducted extensive global operations in support of U.S. national security priorities, including multiple deployments on embedded assignments with U.S. Special Operations Command in Afghanistan and the Horn of Africa. In addition, he has first-hand experience tackling the challenges encountered at the intersection of intelligence and cyber-technology. Jeff earned a Bachelor of Science degree from Hampton University and a Master of Public Administration from the Harvard Kennedy School of Government. He is currently a member of the Council on Foreign Relations and a Fellow with the Intelligence Project at Harvard's Belfer Center for Science and International Affairs. Mr. Fields volunteers as a mentor with the non-profit Girl Security, and he is an unabashed hip-hop head and a fan of the opera.

Ritwik Gupta is the Deputy Technical Director for Autonomy at the Defense Innovation Unit. He oversees DIU's technical efforts in the areas of ground, aerial, and maritime autonomy. Ritwik's background is in artificial intelligence for humanitarian assistance and disaster response. His work has been deployed widely around the world in areas such as automated damage assessment and dark vessel detection. Ritwik is a PhD student at UC Berkeley in AI and Public Policy and is a Fellow at Berkeley's Center for Security in Politics.

Chris Hoofnagle is Professor of Law in Residence at the University of California, Berkeley. An elected member of the American Law Institute, he advises emerging technology companies in defense, intelligence, and law enforcement contexts. He is of counsel to Gunderson Dettmer LLP.

Special Agent **Aleksandr Kobzanets** became an FBI agent in 2005 and has extensive experience working organized crime and national security investigations. From 2020 until the end of 2022, Alex served as the FBI's Assistant Legal Attaché in Ukraine. In this capacity, he worked very closely with the Ukrainian cyber counterparts on all cyber matters.

Elaine Korzak is currently a Postdoctoral Scholar at the UC Berkeley Center for Long-Term Cybersecurity. Her PhD, which she earned from the Department of War Studies at King's College London in 2014, examined the applicability and adequacy of international law in regulating the use of cyberattacks by states. Her research interests span a number of legal and policy aspects of cybersecurity, including norms and international law in cyberspace, cyber capacity-building, and international export control regimes seeking to curb the proliferation of cyber weapons.

Raymond Kuo is the inaugural Director of the Taiwan Policy Initiative and a Senior Political Scientist at the RAND Corporation. He is an expert on international security, international order, and East Asia. Raymond's first book – *Following the Leader: International Order, Alliance Strategies, and Emulation* – explains how military alliance strategies generate international order. His second book – *Contests of Initiative: Confronting China's Gray Zone Strategy* – recommends three courses of action for the U.S. to defeat and deter Chinese coercion in the East and South China Seas.

Tim Mather is a Partner at Fortium Partners, an IT consulting firm, where he has assisted many clients with security issues (including ransomware remediation), developing security programs, and security evaluations. Additionally, he advises several cybersecurity start-ups on their product strategies and marketing, and he advises a venture capital firm on investments in cybersecurity start-ups. Tim has three times served as an enterprise CISO in the tech industry.

Nick Merrill directs the Daylight Lab at the UC Berkeley Center for Long-Term Cybersecurity. His work is built on a simple observation: that security is difficult to practice in part because it's difficult to understand. His lab's work shifts the way people understand and identify the harms of technology—and expands the populations able to do so. By generating novel tools, practices, and representations, he works to make "security" specific and actionable to those who need it. Nick has published over a dozen articles in peer-reviewed venues such as ACM CHI, DIS, and CSCW.

Janet Napolitano is a Professor of Public Policy at the Goldman School of Public Policy, and the Founder and Faculty Director of the Center for Security in Politics at UC Berkeley. She served as the 20th president of the University of California, the nation's largest public research university with ten campuses, five medical centers, three affiliated national laboratories, and a statewide agriculture and natural resources program. Prior to joining the University of California, Professor Napolitano served as Secretary of Homeland Security from 2009 to 2013. She is a former two-term Governor of Arizona, a former Attorney General of Arizona, and a former U.S. Attorney for the District of Arizona. Napolitano is the current President of the Truman Scholarship Foundation and serves as a board member for RAND Corporation, VIR Biotechnologies, Zoom, the International Rescue Committee, and the Council on Foreign Relations. She also serves on the Council of the American Law Institute Advisory Committee. In 2022, President Biden appointed Napolitano to the President's Intelligence Advisory Board. In 2019, Napolitano published *How Safe Are We? Homeland Security Since 9/11*. Professor Napolitano earned her B.S. degree, summa cum laude, in Political Science from Santa Clara University, and her J.D. from the University of Virginia. She is based in Berkeley, California.

Andrew W. Reddie is an Associate Research Professor at the UC Berkeley Goldman School of Public Policy, and Founder of the Berkeley Risk and Security Lab. His research at the intersection of technology, politics, and security examines how technology shapes international order—with a focus on nuclear weapons policy, cybersecurity, AI governance, and innovation.

Hungdah Su is Dean of Social Sciences and Jean Monnet Chair Professor of Political Science at National Taiwan University (NTU). He currently serves as the Director-General of European Union Centre in Taiwan, and is an author of editorials for *The Economic Daily.* His research interests focus on the European integration, transnational cooperation, and Asian regionalism. His most recent publication was *European Dream and Reluctant Integration in the 21st Century: Lessons for*

Ongoing Asian Regionalism (NTU Press, 2020).

Graham Webster is a research scholar in the Program on Geopolitics, Technology, and Governance at Stanford University, where he leads the DigiChina Project. Webster also writes the independent “Here It Comes” e-mail newsletter. He was previously a senior fellow and lecturer at Yale Law School, where he was responsible for the Paul Tsai China Center’s U.S.–China Track 2 dialogues for five years before leading programming on cyberspace and high-tech issues. In the past, he wrote a CNET News blog on technology and society from Beijing, worked at the Center for American Progress, and taught East Asian politics at NYU’s Center for Global Affairs. Graham holds a master’s degree in East Asian studies from Harvard University and a bachelor’s degree in journalism from Northwestern University. He is based in Oakland, California.

Cyber Defending Taiwan:

Lessons from Ukraine

Date: Friday, September 29, 2023

Time: 10:00am to 3:00pm (PT)

Location: Great Hall , Bancroft Hotel, 2680 Bancroft Way, Berkeley, CA

Host: UC Berkeley Center for Long-Term Cybersecurity

Deepening Taiwan's defense and resilience in the cyber domain is key to advancing diplomatic solutions to the rising geopolitical tensions with China in the region.

This one-day conference engaging private, public, and academic leaders will focus on increasing the resilience of Taiwan to threats and vulnerabilities in the cyber domain and beyond. In the process, the workshop engages with the lessons learned from recent history—drawing on the recent Russian invasion of Ukraine.

Co-sponsored by:

- Berkeley Risk and Security Lab
- Institute of International Studies
- Human Rights Center
- Center for Security in Politics
- Berkeley APEC Study Center
- Korea Law Center
- The Miller Institute for Global Challenges and the Law
- The Alexander Hamilton Society

Featuring

10:00 – 10:05am – Welcome and Introductory Remarks

Professor Chris Hoofnagle
Conference Chair

Faculty Director
Center for Long-Term Cybersecurity

Professor of Law in Residence
UC Berkeley School of Law

Agenda

10:05 – 11:15am – Session 1: Cyberattacks in the Ukrainian Invasion

Looking back at the February 2022 Russian invasion of Ukraine and previous Russian cyberattacks, this session will explore what kinds of signposts might exist before aggression against Taiwan.

Confirmed Panelists:

- Gil Baram – Postdoctoral Scholar, UC Berkeley Center for Long-Term Cybersecurity
- Lindsay Freeman – Technology, Law, and Policy Director, Human Rights Center, UC Berkeley School of Law
- Aleksandr Kobzanets – Special Agent, FBI
- Elaine Korzak – Postdoctoral Scholar, UC Berkeley Center for Long-Term Cybersecurity
- Andrew Reddie – Founder, Berkeley Risk and Security Lab; Associate Research Professor, UC Berkeley Goldman School of Public Policy

Gil Baram
Center for Long-Term Cybersecurity

Lindsay Freeman
Human Rights Center

Aleksandr Kobzanets
FBI

Elaine Korzak
Center for Long-Term Cybersecurity

Andrew Reddie
Berkeley Risk and Security Lab
Moderator

11:15am – 12:15pm – Session 2: The Taiwan Context

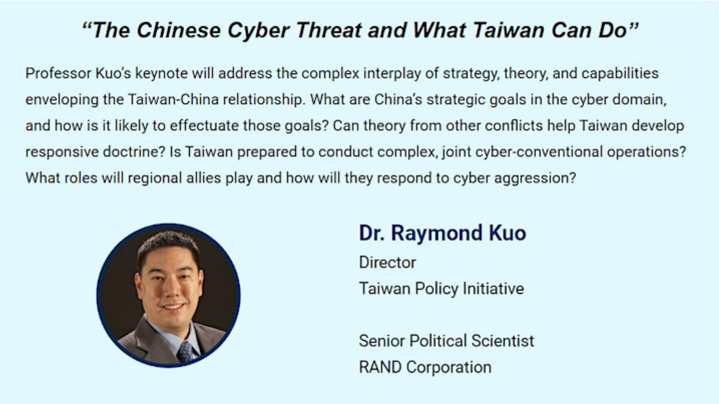
This session transitions to the Taiwan security context to better understand its posture with China as a competitor. What are the characteristics of Taiwan's internet infrastructure and how might it resist physical or logical cyberattack? How has the larger technology competition strategy between the US and China affected Taiwan? How might China's prowess in outer space affected its cyber posture with regard to Taiwan?

Confirmed Panelists:

- Vinod Aggarwal – Director, Berkeley Asia Pacific Economic Cooperation Study Center; Professor, UC Berkeley Travers Department of Political Science
- Benjamin Bahney – Senior Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory
- Graham Webster – Research Scholar, DigiChina Project, Program on Geopolitics, Technology, and Governance at Stanford University
- Nick Merrill – Director, Daylight Security Research Lab, UC Berkeley Center for Long-Term Cybersecurity

Benjamin Bahney
Lawrence Livermore National Laboratory
Nick Merrill
Center for Long-Term Cybersecurity
Graham Webster
Stanford University Cyber Policy Center
Vinod Aggarwal
Berkeley APEC Study Center
Moderator

12:30 – 1:00pm – Lunch Keynote



"The Chinese Cyber Threat and What Taiwan Can Do"

Professor Kuo's keynote will address the complex interplay of strategy, theory, and capabilities enveloping the Taiwan-China relationship. What are China's strategic goals in the cyber domain, and how is it likely to effectuate those goals? Can theory from other conflicts help Taiwan develop responsive doctrine? Is Taiwan prepared to conduct complex, joint cyber-conventional operations? What roles will regional allies play and how will they respond to cyber aggression?

Dr. Raymond Kuo
Director
Taiwan Policy Initiative

Senior Political Scientist
RAND Corporation

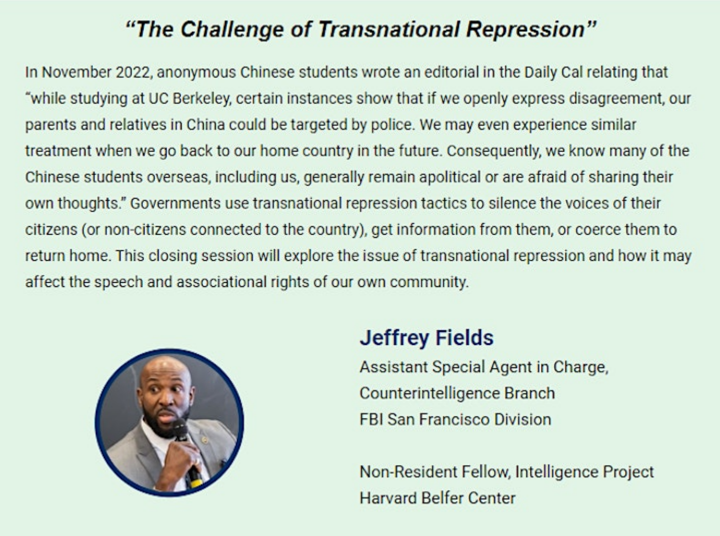
1:25 – 2:25pm – Session 3: Securing Freedom for Taiwan

Private ownership of internet infrastructure makes corporations key partners in security. This forward-looking session analyzes what the public and private sector should be doing now and in the next 2–3 years to secure Taiwan.

Confirmed Panelists:

- Ritwik Gupta – Deputy Technical Director for Autonomy, Defense Innovation Unit
- Hung-dah Su – Dean, College of Social Sciences; Professor, Department of Political Science, National Taiwan University
- Tim Mather – Partner and vCISO, Fortium Partners
- Janet Napolitano – Director, Center for Security in Politics; Professor, UC Berkeley Goldman School of Public Policy

2:30 – 3:00pm – Closing Keynote



"The Challenge of Transnational Repression"

In November 2022, anonymous Chinese students wrote an editorial in the Daily Cal relating that "while studying at UC Berkeley, certain instances show that if we openly express disagreement, our parents and relatives in China could be targeted by police. We may even experience similar treatment when we go back to our home country in the future. Consequently, we know many of the Chinese students overseas, including us, generally remain apolitical or are afraid of sharing their own thoughts." Governments use transnational repression tactics to silence the voices of their citizens (or non-citizens connected to the country), get information from them, or coerce them to return home. This closing session will explore the issue of transnational repression and how it may affect the speech and associational rights of our own community.

Jeffrey Fields

Assistant Special Agent in Charge,
Counterintelligence Branch
FBI San Francisco Division

Non-Resident Fellow, Intelligence Project
Harvard Belfer Center

Additional speakers to be announced soon!

Register

Selected literature:

- Gordon, Susan M., Michael G. Mullen, and David Sacks, U.S.-Taiwan Relations in a New Era:vResponding to a More Assertive China , CFR Task Force No. 81 (2023)
- Huang, Hsini & Li, Tien-Shen (2018) A centralised cybersecurity strategy for Taiwan , Journal of Cyber Policy, 3:3, 344-362, DOI: 10.1080/23738871.2018.1553987
- Aggarwal, Vinod K. & Andrew W. Reddie (2018) Comparative industrial policy and cybersecurity: a framework for analysis , Journal of Cyber Policy, 3:3, 291-305, DOI: 10.1080/23738871.2018.1553989
- Microsoft Digital Security Unit, An overview of Russia's cyberattack activity in Ukraine (April 2022)
- Anonymous Chinese Students, The Poster Movement: A lonely protest in Beijing echoed by politically awakening Chinese students overseas, The Daily Cal, Nov. 17, 2022: https://www.dailycal.org/2022/11/17/the-poster-movement-a-lonely-protest-in-beijing-echoed-by-politically-awakening-chinese-students-overseas

Bibliography

Anonymous Chinese Students. "The Poster Movement: A lonely protest in Beijing echoed by politically awakening Chinese students overseas". In: *Daily Cal* (Nov. 2022). url: https://dailycal.org/2022/11/17/the-poster-movement-a-lonely-protest-in-beijing-echoed-by-politically-awakening-chinese-students-overseas.

Baram, Gil. "Securing Taiwan's Satellite Infrastructure Against China's Reach". In: *LawFare* (2023).

Bartles, Charles K. "Getting gerasimov right". In: *Military Review* 96.1 (2016), pp. 30–38. url: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf.

Defense Intelligence Agency. *Challenges to Security in Space*. Tech. rep. 2022. url: https://perma.cc/5HKU-VM6Z.

FBI. *Threat Intimidation Guide*. url: https://www.fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

— *Transnational Repression*. url: https://www.fbi.gov/investigate/counterintelligence/transnational-repression.

Gerasimov, Valery. "The value of science in prediction". In: *Military-Industrial Kurier* 27 (2013).

Heuer, Richards J. *Psychology of intelligence analysis*. Center for the Study of Intelligence, 1999. url: https://perma.cc/N534-CYVP.

Hogeveen, Bart. "The UN norms of responsible state behaviour in cyberspace". In: (2022).

Liang, Qiao and Wang Xiangsui. *Unrestricted warfare*. PLA Literature and Arts Publishing House, 1999. url: https://www.c4i.org/unrestricted.pdf.

Merrill, Nick and Tejas N. Narechania. "Inside the Internet". In: *Duke Law Journal Online* 73 (2023).

Rid, Thomas. "Cyber War Will Not Take Place". In: *Journal of Strategic Studies* 35.1 (2012), pp. 5–32.

Schake, Kori and Allison Schwartz. *Defending Taiwan: Essays on Deterrence, Alliances, and War*. AEI: American Enterprise Institute for Public Policy Research, 2023. url: `https://www.defendingtaiwan.com/`.

CLTC
Center for Long-Term
Cybersecurity
UC Berkeley

Center for Long Term Cybersecurity
Sutardja Dai Hall, Berkeley, CA 94720
cltc.berkeley.edu