# HYBRID THREATS IN BALTICS AND TAIWAN:

## COMMONALITIES, RISKS AND LESSONS FOR SMALL DEMOCRACIES

LIIA LATVIAN INSTITUTE OF
INTERNATIONAL AFFAIRS

THE ASIA PROGRAMME
ĀZIJAS PROGRAMMA

The publication “Commonalities, Risks and Lessons for Small Democracies: Hybrid Threats in Baltics and Taiwan” gathers a group of leading academics and researchers to provide a fresh and current overview of the threats that have proven to be challenging for small democracies. Authors’ contributions go beyond just pointing out the issues. They assess the institutions responsible for managing the risks and talk about both existing and desirable solutions.

This project is managed by the Latvian Institute of International Affairs and supported by the Taipei Mission in the Republic of Latvia.

TAIPEI MISSION
IN THE REPUBLIC OF LATVIA

**Editors:** Andris Sprūds, Una Aleksandra Bērziņa-Čerenkova, Sintija Broka
**Authors:** J. Michael Cole, Ivo Juurvee, Elina Lange-Ionatamišvili, Chia-yi Lee, Hsuan-Yu (Shane) Lin, Vida Macikenaite, Louis Wierenga, Charles K.S. Wu, Yao-Yuan Yeh

**Cover design:** Shutterstock
**Layout:** Oskars Stalidzāns

The opinions expressed here are those of the authors and do not necessarily reflect the position of the Latvian Institute of International Affairs, any of the sponsors, or any governmental entity. The articles do not necessarily reflect the positions of the institutions with which the authors are affiliated with.

# TABLE OF CONTENTS

## SOCIETAL RESILIENCE AND POLITICAL LEGITIMACY

## ENERGY AND CRITICAL INFRASTRUCTURE SECURITY

## CYBERSECURITY

## STRATEGIC COMMUNICATION

# NOTE FROM THE EDITORS

**ANDRIS SPRŪDS**
Director of the Latvian Institute of International Affairs
**UNA ALEKSANDRA BĒRZIŅA ČERENKOVA**
Head of the Asia program at the Latvian Institute of International Affairs
**SINTIJA BROKA**
Researcher at the Latvian Institute of International Affairs

The year 2022 brings the globe into a period of what could be described with the oxymoron "stable uncertainty". Societies around the world are adapting to living their lives and making decisions against the backdrop of the ever-developing COVID-19 pandemic, and the constant lingering feeling of not knowing what tomorrow holds is neither new nor shocking anymore. The conundrum of "stable uncertainty", however, exacerbates and facilitates other diverse challenges, to which we commonly refer as hybrid threats.

The Baltics as well as Taiwan have been facing uncertainties caused by risks to political legitimacy, societal resilience, critical infrastructure, energy security, and cyber security long before the world went into lockdown – and long enough to have developed a certain resilience. It is a resilience that stems from unique, but translatable experiences of small, yet resourceful democracies. The goal of the Latvian Institute of International Affairs publication "Commonalities, risks, and lessons for small democracies: hybrid threats in Baltics and Taiwan" is to take stock of these experiences and their regional manifestations, to draw parallels between the threats that caused them, to map the risks we're still facing, and to present wider lessons based both on the successes and tribulations of the Baltic states and Taiwan. The volume is designed to provide an overview of how the Baltic states of Lithuania, Latvia and Estonia on one side and Taiwan on the other face, combat and conceptualize hybrid threats.

This publication is possible thanks to the support of the Taipei Mission in the Republic of Latvia. The book has gathered a group of leading academics and researchers to provide a fresh and current overview of the threats that have proven to be challenging for small democracies. It is important to note that the contributions go beyond just pointing out the issues – the chapters assess the institutions responsible for managing the risks and talk about the solutions, both existing and desirable ones.

Vida Macikenaite, Assistant Professor at the International University of Japan, in her article on societal resilience in the Baltic states reveals that new challenges have emerged recently, even though Russia is perceived as the key source of hybrid threats in the information and cyber domains. She concludes that further enhancing societal resilience is the key to strengthening Baltic states' capacity to cope with hybrid threats.

A collaboration between Yao-Yuan Yeh, Associate Professor of International Studies University of St. Thomas, Charles K.S. Wu, Assistant Professor, Department of Political Science and Criminal Justice, University of South Alabama, and Hsuan-Yu (Shane) Lin, Pre-doctoral Research Fellow, Fairbank Center, Harvard University, brings an analysis of political legitimacy and trust in Taiwan. The authors describe how Taiwanese politics is still being impacted by the polarization of various issues, despite its high regard for democratic values. This is most notably witnessed in its relations with China. Their conclusion – increasing polarization could weaken the public's trust in the government.

The similarities in the social reactions between the Baltic States and Taiwan to polarizing issues are hard to ignore. The conclusion is that increasing societal resilience to curb erosion from within is an ever-present calculation for small democracies.

In his chapter on energy and critical infrastructure security, Ivo Juurvee, Head of Security & Resilience Programme at ICDS, points out that the most critical infrastructure systems for modern societies, including the Baltic states, are power supply and IT systems. Ivo Jurvee indicates that the

Baltic cyber expertise has already benefitted democratic countries across the globe. Chia-yi Lee, Associate Professor at the Department of Diplomacy, National Chengchi University, makes a similar conclusion. She demonstrates the proximity of the Baltic and Taiwanese experiences, as she notes the vulnerability of energy security in Taiwan caused by reliance on imports. Chia-yi Lee further argues the government needs to update the cyberspace regulation legislation. This is necessary to maintain the balance between cyberspace protection and personal freedom.

Louis Wierenga is a Junior Research Fellow in Comparative Politics at the Johan Skytte Institute of Political Studies, University of Tartu and Lecturer in International Relations at the Baltic Defence College. Previously he has held guest fellowships at Uppsala University's IRES (Institute for Russian and Eurasian Studies), Sodertorn University's Department of Political Science; and with the Chair of Comparative Politics at European University Viadrina Frankfurt (Oder). Louis has also held guest lecturer positions at the University of Latvia and the Tallinn University of Technology (TalTech). Louis's research interest include populist radical right parties - specifically leadership and party structure, social media and discursive opportunity structures, youth organizations, transnational networks, foreign policy, and social movement parties and metapolitical actors and their engagements between ideology and party structures.

The team of Yao-Yuan Yeh, Charles K.S. Wu, and Hsuan-Yu (Shane) Lin is also behind the article on Taiwan's cybersecurity. The authors provide an overview of the development, as well as risks and challenges of Taiwan's cybersecurity structure at the government level. Yeh, Wu, and Lin call for the government to attract high-level talents, boost public-private partnerships, improve collaboration with international partners, and increase public awareness of cybersecurity.

In her contribution on the role of strategic communications in preventing hybrid threats in the Baltic countries, Elīna Lange-Ionatamišvili, senior expert at the NATO Strategic Communications Centre of Excellence and King's College London War Studies Department PhD student, explains how strategic communications can be instrumental in countering cognitive warfare. The author contends the significance of long-term policies that strengthen democracies, economies and societal cohesion is vital for resisting Russia's cognitive warfare against the Baltics. In the concluding chapter, J. Michael Cole, senior fellow with the Global Taiwan Institute in Washington, D.C., and research fellow with the Prospect Foundation in Taipei, presents an analysis of the effects of Beijing's "hybrid warfare" against Taiwan. Cole argues Taiwan's strategic communications strategy must move beyond a reactive approach. The approach should aim at shaping the environment and global discourse in its favour. J. Michael Cole and Elīna Lange-Ionatamišvili make a parallel conclusion – playing narrative catch-up is not enough for a comprehensive strategic communications strategy, be it in Riga, Vilnius, Tallinn or Taipei.

We hope that the reader's main takeaway will be an enriching and empowering one, while examining both risks and opportunities in this volume. It is not the size or the might that determines resilience in the new hybrid setting. Regardless of geographical, political and historical differences between the Baltic states and Taiwan, the cases share many commonalities, and, more importantly, their experiences can be applied for the benefit of small democracies facing hybrid threats in other regions of the world. It is this kind of experience sharing across regions, note comparing in the face of similar tasks, and an open conversation about hybrid threats that involves academics, think-tankers, practitioners and wider societal stakeholders that is essential for us to be able to steer through the times of "stable uncertainty" – and, more importantly, to shield us from whatever the future holds once the uncertainty is no longer stable.

# SOCIETAL RESILIENCE AND POLITICAL LEGITIMACY

# SOCIETAL RESILIENCE AND SOCIETAL ETHNIC CONSOLIDATION: THE CASE OF THE BALTIC STATES

VIDA MACIKENAITE
Assistant Professor at the International University of Japan

This article discusses the major hybrid threats faced by the three Baltic states – Estonia, Latvia, and Lithuania – that gained independence from the Soviet Union only three decades ago. The security situation in the region has significantly deteriorated since 2014, but the probability of conventional warfare is generally regarded to be low. Instead, these three small democracies are exposed to hybrid threats that often target social cohesion and seek to exploit ethnic divisions in society. Understanding those threats and major vulnerabilities in the case of the Baltic states may offer some important lessons for other countries.

There is no single, universally agreed definition of hybrid threats, considering that a wide range of activities falls under this term. Moreover, hybrid threats evolve constantly and new means in hybrid warfare emerge. Building on the description offered in the *Joint Framework on Countering Hybrid Threats,*[1] the European Centre of Excellence for Countering Hybrid Threats defines hybrid threats as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities."[2] Hybrid threats often seek to undermine fundamental democratic values and liberties, which is a challenge for the relatively young democracies of the three Baltic states.

The following analysis first offers a brief overview of the development of the topic of hybrid threats in Estonia, Latvia and Lithuania. It then examines the major challenges that the three countries face. A wide range of means and activities are conducted across different domains, but the Baltic states have suffered from adverse influence activities mostly in the information and cyber security domains. The final part of the article presents further policy recommendations on how the small democracies in the Baltics could strengthen their capacity to cope with hybrid threats, with a major focus on societal resilience.

## THE EMERGENCE OF THE HYBRID THREAT DISCOURSE IN THE BALTIC STATES

In recent years, hybrid threats have been one of the dominant security-related topics in the EU and NATO. In April 2016, the EU adopted *Joint Framework on Countering Hybrid Threats*, laying a foundation for a coordinated response to hybrid threats at the EU level. NATO has had a strategy for countering hybrid warfare since 2015. While these might appear to be relatively new developments, hybrid methods of warfare have long been used to destabilize adversaries. But in recent years, the scale and intensity of hybrid attacks have been unprecedented, mainly due to rapid technological change and global interconnectivity.

From the perspective of the Baltic states, the development of hybrid threats-related policies at the EU or NATO level has been a natural effect of the changing security landscape in Europe, especially the rapidly deteriorating relations between the West and Russia. The issue of hybrid warfare or hybrid threats came into the spotlight in the region after Russia annexed Crimea in March 2014 and subsequently became involved in the military conflict in Eastern Ukraine. These events rang an alarm bell for Estonia, Latvia and Lithuania drawing their attention to the level of threat that Russia might be posing.[3]

In the immediate aftermath of the Ukraine crisis outbreak, different hybrid attack scenarios against one of the three Baltic states were envisaged, e.g., Russia's attempt to overtake Narva, a city in the eastern extreme point of Estonia, where more than 80 per cent[4] of the population are ethnic Russians;[5] or the so-called *little green men*, armed soldiers without insignia that were seen in Crimea in March 2014, entering Latgale, the region in Latvia's east;[6] or Russia creating an incident linked to Kaliningrad – the Russian enclave on the Baltic sea wedged between Lithuania and Poland. These scenarios included Russia sending troops to "restore order" in case of an uprising in Kaliningrad, or sabotaging the train lines across Lithuania that serve as a vital transit corridor from Russia.[7] It was regarded that Russia could use the same pretext as in Ukraine, i.e., protection of the Russian-speaking minorities, to target one of the countries in the region, or rely on state-controlled Russian TV channels widely watched by ethnic Russians in the Baltics to spread propaganda and fuel grievances.

On the other hand, it would be inaccurate to argue that the Baltic states became aware of the hybrid threats they face only in 2014. Then, the level of alarm was indeed unprecedented, but the Baltic states had long been aware of the prevalent risks. Estonian security agencies had reported on Russia's attempts to escalate a local conflict on different occasions or to use the so-called compatriot policy of Russians living abroad as early as the 2000s.[8] Further, Russia's information warfare also had been brought to public attention. In 2004, the Estonian security agency observed a turning point in the contents of Russia's information attacks: "[i]f the earlier anti-Estonia articles and statements were above all intended for Russia's citizens and the Russian-speaking population of the neighbouring countries, then recently attempts to influence the opinion of the decision-makers of the third countries (first of all West-European states and the USA) about Estonia, Latvia and Lithuania in negative direction have increased."[9]

2007 marked a turning point, as the actual extent of the hybrid threats that the Baltic states face became evident in Estonia. The country was hit by a series of cyber-attacks stretching over a twenty-two-day period and directed at government servers, banks and essential digital infrastructure. These attacks were dubbed by the media to be the world's first cyber-war.[10] The attacks occurred when Estonia was in an intensive row with Russia over the relocation of a Soviet-era war memorial from the centre of Tallinn to a military cemetery. Although Kremlin has denied its involvement, the attacks were carried out from servers in Russia. A series of investigations suggested that these attacks were politically motivated.[11] The decision to relocate the statue was followed by two nights of rioting in Tallinn, something Estonia's capital had never witnessed before. Some reports later concluded that it was "an early case of a hybrid conflict," because the difference in interpretations of history by Estonians and by Russian-speakers in Estonian society was exploited to sow discontent, and the crisis was fanned by the simultaneous use of diplomacy, fake news on social and traditional media, economic pressure and cyber-attacks.[12]

Over the three decades following the independence from the Soviet Union, the Baltic states have been identifying Russia to be the main source of threat. Nonetheless, recently, new sources and tools of hybrid threats have emerged. First, the awareness among the countries' intelligence communities of the threats posed by China has been growing. The initial signs appeared in early 2018, when Lithuanian security services identified hostile cyber activities from China along with North Korea and Iran against Lithuanian state institutions and its energy sector.[13] In 2019, Latvia's security and intelligence service first included China in its annual report on the previous year pointing at cyber operations aimed at obtaining intelligence data – mainly through economic intelligence.[14] The Estonian security service pointed to Chinese intelligence attempts to recruit EU citizens.[15] In 2020, Lithuania paid considerably more attention to China as a potential threat, mentioning attempts to gather technical intelligence on Lithuanian information systems and gain access to critical infrastructure.[16]

Next, Latvia and Lithuania experienced new hybrid warfare tools for the first time. In spring 2021, Lithuania and Latvia faced an influx of irregular migrants at their borders with Belarus. In Lithuania and beyond it is regarded that the Belarusian regime is manipulating the crisis to put political pressure on the EU.[17] The European Commission defined the situation as a hybrid attack by Belarus.[18]

While Belarus was noted for its intelligence activities in the two countries earlier, the influx of migrants is a new challenge for the region. The number of irregular arrivals to Lithuania through the border with Belarus was estimated at 4115 until August 2021, the yearly number increasing 110 times compared to 2019. Reportedly, in July 2021 alone the number of irregular migrants in one day was close to the number for the whole years of 2020 and 2019 combined.[19] Similarly, Latvia witnessed a significantly higher number of migrants in 2021 at its border with Belarus, eventually prompting the Latvian government to declare a state of emergency along the border in August 2021.

## PRIMARY CHALLENGES, RISKS AND LESSONS LEARNED

Hybrid threats involve a wide range of ever-expanding activities across different domains. Challenges the Baltic states have faced vary, but the major risk has been associated with Russia's non-military influence activities, which employ political, diplomatic, legal or information tools. These countries are also exposed to hybrid warfare occurring in cyber-space.

A long-term concern has been Russia's so-called compatriot policy. Its officially stated goal is to support Russians living abroad, including the defence of their interests and rights in their place of residence. In practice, it is regarded that Russia involves compatriot organisations to influence the domestic politics of the Baltic states, gather intelligence, and also exercise soft power. It actively promotes the narrative of the disadvantageous situation of ethnic Russians there and thus instigates opposition between Russian-speaking residents and central authorities. Further, compatriot organizations are exploited to organize various events promoting Russia's positive image and a particular historical events narrative, serving Russia's information policy purposes.

Generally, it is widely regarded that Russia's information policy is coordinated at the highest level and Kremlin uses it as an instrument of influence against foreign countries.[20] Information operations are often implemented through a targeted dissemination of propaganda and disinformation. Its purposes include strengthening mistrust in state institutions and military forces, undermining relations with other states, and discrediting NATO forces deployed in the region. In addition, historic memory is often placed at the centre of propaganda and disinformation, aimed at distorting the countries' historical memory and weakening the national identity. The particular historical narrative is very important to Kremlin, thus the financing of propaganda and promotion of history is on the rise.[21]

Russia increasingly adopts legal means and applies them extraterritorially to advance its view of history abroad. For example, "the Russian Investigative Committee brought criminal charges *in absentia* against three Lithuanian judges, who had been investigating the 13 January 1991 Soviet aggression case, and put them on the international wanted list."[22] Furthermore, Russia has established criminal liability for the destruction of monuments of Soviet soldiers abroad, and the Investigative Committee has already launched several investigations.[23]

However, most often influence is exerted through various public information channels. The Russian Embassy in Latvia was said to be paying for articles in Russian-language media, which are published without any indications that the content is sponsored and by whom.[24] Cyber-attacks are also increasingly often used to place fake news articles in the local media. On the other hand, it would be an oversimplification to argue that Russia's influence is exercised in such a straightforward manner. For example, in 2014, Lithuanian security services noted that Lithuanian citizens and organizations that present themselves as Eurosceptics or nationalists are used to implement Russian interests, e.g., by promoting an image that local civil society groups in the region also support the ideas and values that are in line with Russian foreign policy goals.[25]

The Baltic states regularly face challenges in the information field, and ethnic minorities are especially susceptible to such information warfare. Russian-speaking audiences in Latvia and Estonia have been targeted by Russia's information operations via social media, its state-owned television platforms and newspapers, and other agents of influence.[26] In Lithuania, Russian and Polish ethnic groups have been the target of such influence. A study by the Eastern European Study Center based in Vilnius has found that Russian media sources are very popular among Polish and Russian ethnic groups of Lithuania. Both ethnic groups in Lithuania most often, i.e., daily, watch Russian television (56,7% and 41,6% of respondents respectively), while only around 11% of both groups watch the national broadcaster LRT daily. In comparison, only 13,9% of all respondents in the survey said they watch Russian television daily, while 43,1% responded that they never watch Russian TV channels.[27] Television is still relatively popular, providing an easily-available channel to spread disinformation and shape the public narrative, especially among the minority ethnic groups. Russia is seen as interested in fuelling ethnic conflicts within the Polish community in Lithuania and weakening the social cohesion of the country.[28]

Fake news and the spread of disinformation recently have been paired with cyber-attacks.[29] E.g., the website of the Lithuanian State Border Guard Service (VSAT) was hacked in a major cyber-attack in December 2020 to publish a false report alleging that a Polish diplomat had been detained on the border carrying weapons, drugs, and money. This serves as an illustration of Lithuania's Foreign Ministry's statement that there was an increase in attacks "aimed at undermining friendly Lithuanian–Polish relations and pitting the [two] nations against each other."[30] The website of Siauliai Municipality was also hacked at the same time to post a fake article about a local airport that houses NATO's Baltic air policing mission. NATO troops in the region often become the target of disinformation, mainly aimed at decreasing public support for the NATO deployments in the country.

It is estimated that a few dozen cyber-attack cases per year take place in Latvia, carried out mostly for espionage purposes and directed against government institutions in the fields of defence, interior and foreign affairs.[31] In Lithuania, cyber-attacks have been conducted against Lithuania's high-ranking decision-makers as well as public institutions in the domains of foreign affairs, national security, energy and education.[32] In October 2021, the Director of the National Cyber Security Centre under the Lithuanian Ministry of National Defence confirmed that the number of cyber-incidents in 2020 increased by one fourth compared to the previous year. [33] Estonia also saw an increase in the number of cyber-incidents.[34]

After Estonia came under a wave of cyber-attacks lasting for three weeks in spring 2007, the region was quick to learn that cyber-attacks pose a major modern warfare challenge. Already the following year the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn, tasked with conducting cyber defence research and training. All the three Baltic states became the initial signatories of the founding of the centre, along with four other NATO member-states. Estonia became one of the first countries in the world to release a National Cyber Security Strategy as early as 2008. The country also launched a new cyber command division within its military and is internationally advocating for a strong regulatory framework. Lithuania and Latvia followed with their national cyber security strategies in 2011 and 2014 respectively.[35] Estonia and Lithuania rank third and sixth correspondingly on the Global Cybersecurity Index (GCI) list, with Latvia slightly behind ranking 14th.[36] The GCI evaluates legal, technical, organizational, capacity development, and cooperation measures to evaluate the state of a country's cyber security.

Although Russia has long been regarded as the main source of threat to the countries' cyber-security, in recent years, it is no longer limited to this traditional adversary of the Baltic states. China has been added to the list, with Latvian security agencies pointing out that the number of China's cyber operations has been gradually increasing.[37] Also, in Estonia hostile cyber activities have been linked to North Korea and Iran.[38]

After the incidents in Estonia in 2007, the necessity to strengthen cyber-security was obvious. Estonia was quick to learn the lesson and has pioneered the field of cyber-security since then.[39] But the Ukraine crisis in 2014 exposed new gaps in the security of the small democratic countries in Eastern Europe. First, the perception of security provided by NATO membership was soon replaced by the sense of vulnerability in the shadow of new means of warfare. There was a question on the link between a case of a cyber-attack and Article Five. In the case of an invasion by the so-called *little green men*, the challenge to identify those responsible also made a coordinated response difficult or even impossible.

Second, the Baltic states were well aware of their vulnerabilities. With their ethnic groups relatively poorly integrated, Baltic states could easily be susceptible to various influence operations. In Latvia, 25.4% of the population are Russian (in 2017), in Estonia – 29.6% (2011), and in Lithuania Russians and Poles comprise 5.8% and 6.6% of the population respectively (2011).

Finally, the Baltic states were very quick to reconsider the risks associated with their energy security, which became especially pressing after the start of the 2014 Ukraine crisis. The three Baltic states used to be fully dependent on Russia for gas imports mainly due to the remaining Soviet infrastructure.

As a result, Baltic-Russian relations used to be characterised by the factor of acute gas dependence, making the three states vulnerable to price manipulation and cut-offs. The countries have been able to overcome this challenge. In 2014, Lithuania built a liquified natural gas terminal (LNG). The countries have also been able to improve their gas, as well as electricity, connections to Europe under the Baltic energy market interconnection plan (BEMIP) initiative by the EU. As a result, since then, energy security threat percepetion in the Baltic states shifted away from energy dependency on Russia. But in 2020, the State Security Department of Lithuania estimated that Russian energy companies were still seeking to maintain dominance over the Baltic energy markets.[40]

## DISCUSSION AND FURTHER POLICY RECOMMENDATIONS

Long aware of the challenges faced, the Baltic states have implemented a wide spectrum of measures to counter hybrid threats. It would require a separate paper to discuss them in detail, but generally, the measures have been aimed at improving collective situational awareness, preventing, responding to or recovering after attacks.

As hybrid warfare continues to change and new means emerge, it is not always possible to swiftly prevent or respond to hybrid attacks. E.g., Lithuania has sought to prevent society's exposure to adverse information from Russia by limiting Russian content on television. But patterns of media consumption and production are undergoing rapid transformation. Instead of users consuming traditional media, anyone now can create and spread content, which is increasingly difficult to control. Against this background, existing policies would be less effective in the long-term. Further, investment in societal resilience may be the most effective strategy to strengthen Baltic states' ability to cope with hybrid threats, considering that the region is exposed to influence activities by hostile actors that target different social groups.

First, further increasing media literacy demands substantial attention, especially in Latvia and Lithuania. In 2021, according to the *Media Literacy*

*Index*, which measures the potential of European countries to withstand the negative impact of fake news and misinformation due to the quality of education, free media and high trust among people, Estonia ranked 3rd, but Latvia and Lithuania – only 20th and 18th respectively among 35 countries. Media and information literacy education targeting broader segments of society is crucial. Thus, new private initiatives should be encouraged and the already existing ones supported by the state. An example of good practices is Debunk.eu – a private initiative. It is an independent analytical centre and an NGO that researches disinformation in the public space and executes educational media literacy campaigns in Lithuania,[41] created with the purpose of increasing society's resilience to orchestrated disinformation campaigns.

Further, access to independent media and news sources is important, especially for the Russian or Polish ethnic groups living in the Baltic states. On the one hand, it has been argued that it is in the interest of Russia to maintain ethnic divisions in the Baltic states, thus, ethnic group integration is crucial.[42] On the other hand, as a survey in Lithuania has revealed, Polish and Russian ethnic groups live in the Russian cultural and information field. Therefore, while it remains a long-term challenge to integrate ethnic groups and strengthen societal cohesion, in the medium-term, the access of ethnic groups to independent news sources in their language must be assured. Language should not become a mark of division in the society, but instead should be utilized by the state and also private media organizations to deliver accurate and reliable information. The language of ethnic groups can also be used to help recognize propaganda and information warfare, instead of pushing their speakers into the information sphere of hostile states.

Hybrid threats are often aimed at the most vulnerable points of a state. Thus, supporting a well-educated and informed society across all ethnic groups using the means acceptable to them is a fundamental step in countering hybrid threats.

## ENDNOTES

[1] "Joint Framework on Countering Hybrid Threats – A European Union Response", Joint Communication by the European Commission and the High Representative to the European Parliament and the Council, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=SV.

[2] "Hybrid Threats as a Concept", European Centre of Excellence for Countering Hybrid Threats, n.d. Accessed November 4, 2021, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.

[3] Milne R., Foy, H., "NATO Frontline States See Fears over Russia Realized", 31.08.2014, https://www.ft.com/content/13f822e4-30f4-11e4-b2fd-00144feabdc0.

[4] Koval, I., "Narva: The EU's 'Russian' City", Deutsche Welle, 26.05.2019, https://www.dw.com/en/narva-the-eus-russian-city/a-48878744.

[5] Rubin, J., "NATO Fears That This Town Will Be the Epicenter of Conflict With Russia", The Atlantic, 24.01.2019, https://www.theatlantic.com/international/archive/2019/01/narva-scenario-nato-conflict-russia-estonia/581089/.

[6] Mierzejewski-Voznyak, M.G., "Crafting a Strategic Response to Russia: Geopolitical Priorities for Latvia in 2015", Latvian Foreign and Security Policy Yearbook 2015, Sprūds, A., Potjomkina, D., (eds.), The Latvian Institute of International Affairs, 2015, p. 36.

[7] Milne, R., Foy, H., "Baltic Security: Tensions on the Frontier", The Financial Times, 20.10.2014, https://www.ft.com/content/13469356-5829-11e4-b331-00144feab7de.

[8] "Annual Review 2003", Security Police of the Republic of Estonia, 2004, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%20 2003.pdf.

[9] "Annual Review 2004", Security Police of the Republic of Estonia, 2005, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202004.pdf.

[10] Welscher, A., "More than a Virus: Pandemic and Online Security in the Baltic states", Public Broadcasting of Latvia, 12.04.2021, https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/.

[11] Ottis, R., "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008, Academic Publishing Limited, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, p. 163-168.

[12] Mattiisen, M., "The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict," International Centre for Defence and Security, August 2020, https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

[13] "National Threat Assessment 2018", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2018, https://www.vsd.lt/wp-content/uploads/2018/03/ENG.pdf, p. 33.

[14] "Annual Report 2018", Constitution Protection Bureau of the Republic of Latvia, 2019, https://www.sab.gov.lv/files/Public_report_2018.pdf, p. 38.

[15] "Annual Review 2018", The Estonian Internal Security Service, 2019, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202018.pdf.

[16] "National Threat Assessment 2020", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2020, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf, p. 34.

[17] Psara, M., "'Absolutely Unacceptable': Belarus Accused of Using Migrants in its Fight with EU", Euronews, 12.07.2021, https://www.euronews.com/2021/07/12/absolutely-unacceptable-belarus-accused-of-using-migrants-in-its-fight-with-eu.

[18] "Brussels Recognises Migrant Crisis on Belarus Border as Hybrid Attack", BNS, 29.09.2021, https://www.lrt.lt/en/news-in-english/19/1507595/brussels-recognises-migrant-crisis-on-belarus-border-as-hybrid-attack.

[19] "Frequently Asked Questions about Irregular Migrants Detained at the Border with Belarus", Ministry of the Interior of the Republic of Lithuania, last updated August 12, 2021, https://vrm.lrv.lt/en/information-on-irregular-migration.

[20] "National Threat Assessment 2020", Second Investigation Department and the State Security Department, p. 34.

[21] "Annual Report 2019", Constitution Protection Bureau of the Republic of Latvia, 2020, https://www.sab.gov.lv/files/Public_report_2019.pdf, p. 22.

[22] "National Threat Assessment 2021", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2021, https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf, p. 11.

[23] Ibid.

[24] "Annual Report 2019", Constitution Protection Bureau of the Republic of Latvia, 2020, https://www.sab.gov.lv/files/Public_report_2019.pdf, p. 21.

[25] "National Threat Assessment 2015", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2015, https://www.vsd.lt/wp-content/uploads/2016/10/Gresmiu-vertinimas-2014.pdf, p. 15.

[26] Kalniete, S., Pildegovics, T., "Strengthening the EU's Resilience to Hybrid Threats," European View 2021, Vol. 20(1) 23–33, https://doi.org/10.1177/17816858211004648, p. 30.

[27] Jastramskis, M., "Reaction of the Audience: The Impact of Russian Propaganda in Lithuania", in Russian Propaganda: Analysis, Evaluation, Recommendations, Vaišnys, A., Kasčiūnas, L., Jastramskis, M., Keršanskas, V., Buinauskas, D., Kojala, L., Klimanskis, S., Garbačiauskaitė-Budrienė, M., Legatas Š, (eds.), Eastern European Study Center, 2017, https://www.eesc.lt/uploads/news/id987/RESC%20monografija_propaganda.pdf, p. 153.

[28] "National Threat Assessment 2016", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2016, https://www.vsd.lt/wp-content/uploads/2016/10/EN-2015-gresmes.pdf, p. 46.

[29] "Cyberattacks are More Abundant and More Complex, Says Director of the National Cyber Security Centre R. Rainys," Ministry of National Defence of the Republic of Lithuania, 07.10.2021, http://kam.lt/en/news_1098/current_issues/cyberattacks_are_more_abundant_and_more_complex_says_director_of_the_national_cyber_security_centre_r._rainys.html.

[30] "Lithuania under 'Complex Cyber Attack', Says Foreign Ministry," BNS, 10.12.2020, https://www.lrt.lt/en/news-in-english/19/1295923/lithuania-under-complex-cyber-attack-says-foreign-ministry.

[31] "Annual Report 2019", Constitution Protection Bureau of the Republic of Latvia, 2020, https://www.sab.gov.lv/files/Public_report_2019.pdf, p. 26.

[32] "National Threat Assessment 2021", Second Investigation Department under the Ministry of National Defence and the State Security Department of the Republic of Lithuania, 2021, https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf, p. 47.

[33] Cyberattacks are More Abundant.

[34] "Cyber Security in Estonia 2021", Information System Authority of the Republic of Estonia, 2021, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.

[35] "National Cyber Security Strategies - Interactive Map," European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[36] "Global Cybersecurity Index 2020", the International Telecommunication Union (ITU), https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

[37] "Annual Report 2018", Constitution Protection Bureau of the Republic of Latvia, 2019, https://www.sab.gov.lv/files/Public_report_2018.pdf.

[38] "Annual Review 2020-2021", Estonian Internal Security Service, 2021, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202020-2021.pdf, p. 30.

[39] For example, for a detailed account on Estonia's measures in cyber deterrence see Pernik, P., "Cyber Deterrence: A Case Study on Estonia's Policies and Practice", The

European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE Paper 8, 12.10.2021, https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf.

[40] "National Threat Assessment 2020", Second Investigation Department and the State Security Department, p. 5.

[41] Available at Debunk.eu, https://debunk.eu.

[42] "Annual Review 2020-2021", Estonian Internal Security Service, p. 7.

# POLITICAL LEGITIMACY AND TRUST – THE CASE OF TAIWAN

**HSUAN-YU (SHANE) LIN**
Pre-doctoral Research Fellow, Fairbank Center, Harvard University; PhD. Candidate, Department of Politics, University of Virginia

**CHARLES K.S. WU**
Assistant Professor, Department of Political Science and Criminal Justice, University of South Alabama

**YAO-YUAN YEH**
Chair and Associate Professor, Department of International Studies & Modern Languages, University of St. Thomas, Houston

> "The strongest man is never strong enough to be master all the time, unless he transforms force into right and obedience into duty."
> – Rousseau, *The Social Contract & Discourses*[1]

What is political legitimacy? Are sources of political legitimacy different for authoritarian and democratic regimes? In this chapter, we briefly review scholarly work on political legitimacy before turning to the case of Taiwan, whose history and democratic transition reflect political leaders' needs to seek out different sources of political legitimacy from their constituents. After nearly three decades of democratization, despite high regard for democratic values, Taiwanese politics is still being impacted by polarization on various issues, most notably, its relations with China. The increasing polarization challenges this new democratic polity and could weaken the public's trust in the government.

## WHAT IS POLITICAL LEGITIMACY?

How do we understand the term "political legitimacy?" Why do countries try their best to maintain political legitimacy? Scholars in political science have not reached a consensus on the definition of this term.[2] In this chapter, since we do not focus on the debate about the definition of political legitimacy, we define this term in a simple but concrete way. Political legitimacy, in general, refers to the popular acceptance and recognition by the people of the authority of a governing regime.[3] Political legitimacy plays a critical role in the sustainability of a government or a regime since a government/regime without sufficient political legitimacy would encounter internal threats and challenges which could overthrow it. As political legitimacy largely determines the fate of a government or a regime, that is why both democratic and authoritarian governments are sensitive to it.

Where does political legitimacy originate? Again, scholars have different views on the sources of political legitimacy. German sociologist Max Weber argued that there are three types of political legitimacy: traditional legitimacy, charismatic legitimacy, and rational-legal legitimacy.[4] Traditional legitimacy is based on societal norms and habits emphasizing traditional authority's history, which means that the authority's continuous ruling is considered a tradition and this ruling continuity generates legitimacy. Under this legitimacy, people accept a regime's continuous ruling because it is the way society has always been. Charismatic legitimacy is based on a leader's charisma and ideas. The leader's authoritative persona charms and psychologically dominates the people of the society into obeying the leader and the government's ruling. Rational-legal legitimacy, the category we will focus on in this chapter, derives from a system of institutional procedure in which institutions establish and enforce law and order in the public's interest. Rational-legal legitimacy works only when the governed (i.e., the people) trust the government and follow the law.[5]

How do democracies build political legitimacy? Essentially, free, periodic elections and representation help ensure democratic citizens' acceptance of being ruled by an authority. Through elections, people decide whom they want to endorse, giving the endorsed authority the power to govern.

However, as Weber said, democracy is not necessary for establishing political legitimacy.[6] Democracy can backslide. As a result, democratic society may revert to the charismatic and authoritarian government, such as the Nazi Germany of Adolf Hitler.

While authoritarian regimes do not hold free and open elections, they can also build political legitimacy. For them, performance is the first source of political legitimacy. Performance can range from security and safety to economic prosperity, preservation of cultural values, and safeguarding national pride and prestige.[7] In addition, nationalism is also a source for democracies and autocracies to sustain their ruling legitimacy. [8] Nationalist appeals are typically founded upon language, ethnicity, history, or tradition and are employed to create a sense of solidarity among often quite disparate populations. For example, scholars have attributed China's legitimacy to economic growth and nationalism. Pan argues that the Chines government is skilful at rallying nationalist sentiments, and the growing economic prosperity has enhanced the Chinese Communist Party's (CCP) reputation.[9] Authoritarian governments usually safeguard their ruling legitimacy with coercion and suppression, such as cracking down on dissidents and censoring politically sensitive information. These strategies help authoritarian regimes maintain people's willingness to support their ruling and increase people's cost of disobedience.

## SOURCES OF POLITICAL LEGITIMACY IN TAIWAN

Granted that the above discussions focus on ideal types, it will be helpful to examine some examples where both authoritarian and democratic characteristics exist in the same country. Taiwan is an interesting case because it has experience in both authoritarian and democratic political legitimacy. Taiwan's democratization started in 1987; before 1987, it was an authoritarian regime, and after 1987, it gradually became a budding democracy in Asia. Going back in history, when the Republic of China (ROC) government lost the Chinese Civil War to the Chinese Communist Party (CCP) in 1949, the ROC government and its troops, business groups, and refugees fled to the island of Taiwan. That same year, on October 1st, the CCP as the victor of the civil war established the People's Republic of China in the mainland. After the ROC retreated to Taiwan, it started enforcing martial law in Taiwan. The martial law lasted for 38 years, restricting Taiwanese citizens' rights of political participation, freedom of speech, and public gathering until 1987.

During this authoritarian period of the ROC regime, the political legitimacy was based on nationalism and economic prosperity. Wu and Cheng argue that the Nationalist government (or the KMT government) needed a higher degree of legitimacy than its counterparts, such as South Korea.[10] They posit that, first, the ruling group lacked social and political connection with the local society because it had just migrated from the mainland. Second, the tensions between islanders (who had lived on the island before 1949) and newcomers (who migrated to Taiwan with the Nationalist government in 1949) also pushed the Nationalist government to seek "higher" ruling legitimacy. The tension between islanders and newcomers was partially caused by the KMT government's large-scale killing and repression of islanders in 1947.

As Figure 1 shows, Taiwan's economy took off in the late 1960s. Taiwan's outstanding economic performance since the late 1960s provided new political legitimacy for the Nationalist government. The development of Taiwan's economy justified the Nationalist government's authoritarian rule during that

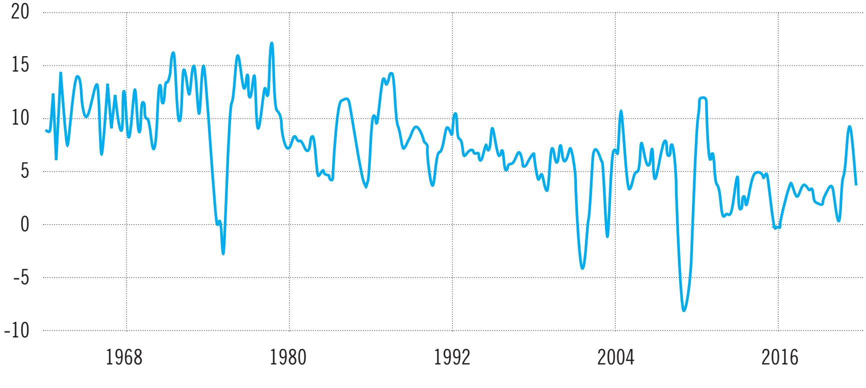


**FIGURE 1. TAIWAN'S GDP GROWTH, 1965–2020.**

Note: The sudden drop in Taiwan's economic growth rate in the 1970s was caused by the oil crisis, but Taiwan's economic growth returned to normal after the crisis.

time.[11] However, as the Taiwanese people were getting more prosperous, they started to demand more political rights from the government.

The seed of democratization was quietly planted during Taiwan's economic take-off. The Tangwai (meaning "people outside the Nationalist party" in Chinese) movement, which later morphed into the major opposition party, the Democratic Progressive Party (DPP), is an example. One goal of this movement was the reform of the Legislative Yuan, Taiwan's legislative body, hoping to introduce new voices into the parliament to supervise the government.

The Tangwai movement started to gain traction in the late 1980s as a series of democratization efforts unfolded. The first one is the establishment of the DPP in 1986, which advocates for Taiwan's independence. The next year, Chiang Ching-kuo, the then-president of the ROC, lifted the martial law on the Taiwan island. With the lifting of martial law, discussing politics or statehood was no longer taboo. People could freely express their opinions about the country and politics, allowing more voices to be heard, noticed, and respected.[12] President Lee Teng-hui, the successor of Chiang Ching-kuo, further deepened Taiwan's democratic reforms. He reformed the Legislative Yuan and abolished the National Assembly, forcing original members of these institutes elected in 1947 to resign. These reforms allowed more Taiwanese to participate in political activities. Since then, especially after the first direct presidential election in 1996, Taiwan has stepped into a period of full democracy.

Behind this successful democratization story is an interesting research puzzle – why did the ruling party, the KMT, decide to democratize the country, a behaviour seemingly undermining the party's grips of power or even survival? While there are several explanations in the literature on institutionalization and democratization of authoritarian regimes,[13] one argument is related to political legitimacy. Huntington argued that authoritarian regimes could confront the erosion of their legitimacy by introducing democracy.[14] One caveat, though, is that the ruling elites must be confident about the result of democratic elections, allowing them to continue to hold power.[15] In Taiwan's case, according to Wu and Cheng, the ruling regime's economic performance, governing experience, and a moderate liberal-inclined opposition were among the factors building the ruling elites' confidence in favourable results of free and open elections.

The results after democratization largely matched KMT's expectations. In the first ten years after Taiwan's democratization, the KMT did perform quite well in most elections. However, the component of political legitimacy for democratic Taiwan has gradually changed following the political landscape change. To be a well-functioning democracy, the new polity needs to have free, open, and fair periodic elections, and the provisions of these political rights are to be scrutinized by its constituents – the Taiwanese people.

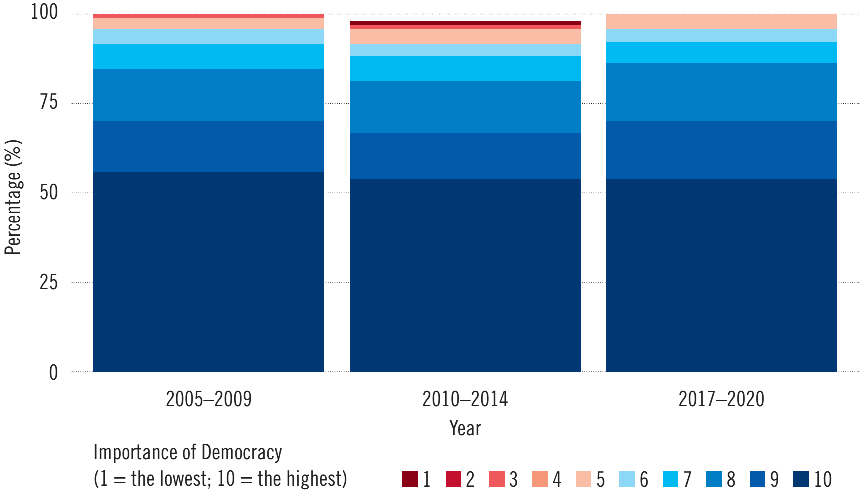


**FIGURE 2. TAIWANESE SUPPORT FOR DEMOCRACY, 2005–2020.** Source: World View Survey.

In fact, yearning for democratic values has been embedded into Taiwanese identity. According to the World View Survey, the popular support for democracy has always been high in Taiwan (see Figure 2). On a 10-point scale, the World View Survey finds that more than 75% of Taiwanese rated the importance of democracy at 7 points or higher from 2005 to 2020. The survey result shows that maintaining democracy is a consensus in the Taiwanese society. Being a democracy means that the government needs to respond to the public's needs and wants. Moreover, people expect their voices to be represented in the government by elected politicians. One potential concern is that if people's preferences are highly divided and polarized, the government may have difficulties satisfying all voters – those who are disgruntled may reduce their political trust in the government and eventually doubt its legitimacy.

Political competition unavoidably leads to the polarization of politics.[16] Polarized politics may "politicize" political legitimacy – people with different political positions may have different views on what composes political legitimacy and which political party owns political legitimacy. The political legitimacy problem, unsurprisingly, appears in Taiwan's politics. Huang points out four dimensions of the political legitimacy problem: Taiwan's future with Mainland China: unification vs. independence; Taiwanese citizens' identity: Chinese vs. Taiwanese; economic dependence on China: less vs. more; and the Nationalist Party's economic legacy vs. the DPP's antiauthoritarian legacy.[17]

The polarization of Taiwan's politics and public opinion is further deepened by Taiwan's political institutions, especially its electoral system, which is a mix of the single-member district plurality (SMDP) and the proportional representation (PR) systems. The SMDP system refers to a system in which one electoral district is represented by only one representative, and the PR system, in general, refers to a system in which the number of seats a political party can obtain is based on the proportion of received party votes in an election. The SMDP system, while giving voters in each district a single and identifiable representative, may over-represent major parties, because their candidates have more resources than candidates of small parties, and are therefore more likely to win SMDP elections. This big-party-friendly electoral system may increase the polarization of Taiwan's politics as it tends to create a two-party system. It would also affect how voters in Taiwan view politics (they are likely to be affected by elite cues from political elites they support). Arguably, polarized political views may eventually challenge the government's ruling legitimacy to some extent as the ruling party is less likely to receive full support from members of the opposing party.

To better understand the challenges facing the Taiwanese government to maintain its political legitimacy, in the next section, we will explore political trust in Taiwan, laying out how political polarization causes political trust deficit and how this deficit brings challenges and opportunities to Taiwan's democracy.

## VARIATION OF POLITICAL TRUST IN TAIWAN

Political trust is defined as one's evaluation of how well a government is operating according to his or her normative expectation; the higher one's evaluation of the government's performance, the higher one's political trust in the government.[18] Political trust is an essential factor determining the effectiveness of a democratic government's functions.[19] This kind of trust is positively associated in countries that provide good governance and care about people's wellbeing and is negatively associated in countries with poor governance and a society divided by social cleavage.[20] Some scholars argue that political trust is correlated with political support. David Easton distinguishes two types of political support: specific and diffuse political support. The former, specific political support, refers to satisfaction with government outputs and the performance of political authorities. The latter, diffuse support, refers to the public's attitude toward regime-level political objects regardless of performance.[21] Some scholars posit that political trust correlates only with specific political support (i.e., satisfaction with government outputs), so "an improvement in incumbent job performance should remedy low levels of political trust."[22] However, some scholars claim that low diffuse political trust may eventually challenge regime legitimacy.[23]

Why does political trust matter? As mentioned, political trust affects democratic governments' possibility to function effectively.[24] Political trust is essential to incentivize public support to overcome collective action problems, making everyone better off through societal cooperation.[25] Political trust also influences public attitudes toward public policies, such as tax[26] and immigration[27]. In Taiwan, we argue that Taiwanese citizens' political trust is largely based on diffuse political support (e.g., people's support for a democratic government). In contrast, their specific political support (e.g., the Taiwanese government's specific policy performance) is subject to political polarization. As Figure 2 shows, Taiwanese people's support for democracy remains quite high no matter which political party, the KMT or the Democratic Progressive Party, rules the government. This high level of support for democracy reflects that Taiwanese people endorse the democratic authority (i.e., the Taiwanese government) to distribute/redistribute resources and govern them.

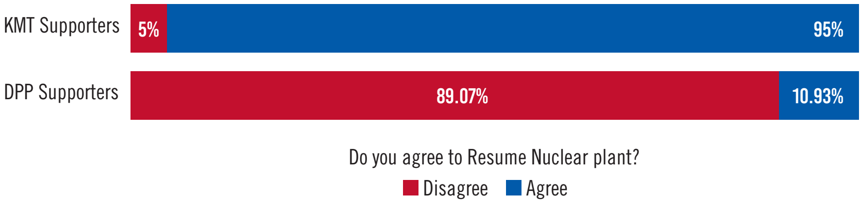


**FIGURE 3. PARTISAN SUPPORT FOR RESUMING THE 4TH NUCLEAR PLANT IN TAIWAN.**

Note: This is an online survey conducted by the FTV News on December 7, 2021 (https://www.facebook.com/ftvnews53/photos/a.10150159841020901/10159461781845901/?type=3). The DPP takes a "disagree" position in this policy issue, and the KMT takes a "agree" position. Most of these parties' supporters took a position consistent with their preferred party. 94.75% of KMT supporters agree to resume the fourth nuclear plant in Taiwan, while only 10.85% of DPP supporters agree to do so. 88.44% of DPP supporters are consistent with the DPP on objecting to the nuclear plant.

However, as Figure 3 shows, Taiwanese people are indeed polarized in specific policies. In an online poll before Taiwan's national referendum in 2021 conducted by the FTV News, one of the major news media outlets, partisans' positions on these policies are mostly consistent with their partisanship. For example, the KMT is in favour of reviving the fourth nuclear power plant, and the majority of KMT supporters (94.75%) supported doing so, too. The DPP is opposed to the proposal, and 88.44% of DPP supporters followed suit.[28] The poll result demonstrates how polarized Taiwan's politics could be and how it affects people's attitudes toward policy preferences regarding specific political support (e.g., support for the DPP administration's terminating the fourth nuclear plant).

How does polarization affect Taiwanese citizens' political trust? Cross-Strait relations is another main polarized issue. The Chinese government claims Taiwan's sovereignty, but Taiwan is a self-governed island, containing all elements of an independent state. China's objections and threats are the main factors preventing Taiwan from exercising its own complete autonomy. How to deal with China has become a highly polarized political topic in Taiwan, and the Taiwanese public's political trust in the Taiwanese government (specific political trust, in particular) is affected by the government's cross-Strait policies.

Taiwan's two major political parties, the Nationalist Party (KMT) and the Democratic Progressive Party (DPP), have opposite positions on cross-Strait issues. The KMT and its political allies (called "pan-blue") support an engagement policy with China by accepting the 1992 Consensus, which argues that there is only one China in the world. While there are few members in the pan-blue camp supporting reunification with mainland China, most of the members do not support Taiwan's independence either. In contrast, the DPP and its political allies (called "pan-green") do not accept the One-China political framework as well as the 1992 Consensus, and many of the members in the pan-green camp support Taiwan's independence.[29]

As political polarization based on cross-Strait relations continues to exist, some may predict that political trust among Taiwanese citizens will not be consolidated across party/ideological lines. However, public opinion surveys reveal a recent development in Taiwanese identity, pointing towards a different possible trajectory. Over the past two decades, the percentage of Taiwanese who self-identify with Taiwanese identity has been steadily increasing, while the percentage of those who hold Chinese identity or dual identity (both Chinese and Taiwanese) has gone in the opposite direction. Now, over 60% of Taiwanese citizens identify as Taiwanese, compared to less than 40% in the 1990s.[30] In addition, the PRC has also continued to threaten Taiwanese citizens that it will not give up its goal of unification, even with force. Constant threats from the PRC in the international arena, the maltreatment of Hong Kong and ethnic minorities, and suppression of freedom, human rights, and democracy are all considered the driving forces for Taiwanese citizens to shy sway from unification under any conditions, including one country or two systems. While cross-Strait relations and policy toward unification/independence taken together still produce the dominant social divide that causes political polarization and undermines political trust in Taiwan, such a divide is likely to fade away as the support for democracy remains strong in the Taiwanese society.

## CONCLUSIONS AND RECOMENDATIONS

This chapter explores the transition of Taiwan's political legitimacy – from authoritarian legitimacy to democratic legitimacy – and the variation of Taiwan's political trust – specific and diffuse political support and political trust. Taiwan was an authoritarian regime before 1987, and the ruling KMT administration relied on nationalism and economic performance to sustain its legitimacy. Democratization began in 1987 – free and periodic elections and representation become Taiwan's new sources of political legitimacy.

Taiwan's democracy has been further consolidated by routine elections. The incumbent and the opposition parties have both ruled the government at least once since 2000, and the power transition has largely been handled peacefully. Although citizens in Taiwan regard democracy as one of the critical factors for these successes, the country, like most democracies, still faces increasing political polarization due to party competition. Cross-Strait issues – especially whether to accept the "one-China" political framework set by the Chinese government – continue to be one of the polarized issues in Taiwan. Thus, despite different opinions on policies reflecting the spirit of democracy, Taiwan still needs to pay close attention to issue-driven polarization that could undermine political trust and democratic political legitimacy.

### ENDNOTES

[1] Rousseau, J.J., "The social contract, & Discourses", Rousseau, J.J., (ed.), London, New York: J.M. Dent & sons, ltd.

[2] Erman, E., Möller, N., "Political Legitimacy for Our World: Where Is Political Realism Going?", The Journal of politics, Vol. 80, No. 2, 2018, https://doi.org/10.1086/694548, p. 525–38.

[3] O'Neil, P.H., Fields, K.J., Share, D., "Essentials of comparative politics with cases", Sixth AP edition, New York: W.W. Norton & Company, 2018.

[4] O'Neil, P.H., Fields, K.J., Share, D., "Essentials of comparative politics with cases", Sixth AP edition, New York: W.W. Norton & Company, 2018.

[5] It is important to note that the causation of political legitimacy and citizens' support for a regime is still unclear in the current scholarly debate. We do not know whether

it is political legitimacy enhancing people's political support, the other way around, or both.

[6] O'Neil, P.H., Fields, K.J., Share, D., "Essentials of comparative politics with cases", Sixth AP edition, New York: W.W. Norton & Company, 2018.

[7] Gilley, B., "The right to rule : how states win and lose legitimacy", New York: Columbia University Press, 2009.

[8] J. Kane, H. Loy, and H. Patapan, "Political Legitimacy in Asia: New Leadership Challenges", 1st ed, New York: Palgrave Macmillan, 2011.

[9] Pan, P. P., "Out of Mao's shadow : the struggle for the soul of a new China", 1st Simon & Schuster hardcover, New York: Simon & Schuster, 2008.

[10] Wu, N., Cheng, T., "Democratization as a Legitimacy Formula: The KMT and Political Change in Taiwan", New York: Palgrave Macmillan US, 2011, p. 239–60.

[11] Ibid.

[12] Wu, J. J., "Taiwan's democratization: forces behind the new momentum", New York: Oxford University Press, 1995.

[13] Meng, A., "Constraining dictatorship: from personalized rule to institutionalized regimes", New York, NY: Cambridge University Press, 2020; Meng, A., "Ruling Parties in Authoritarian Regimes: Rethinking Institutional Strength" British Journal of Political science Vol. 51, No. 2, 2021, https://doi.org/10.1017/S0007123419000115, p. 526–40; Choi, C., Jee, S. H., "Differential Effects of Information and Communication Technology on (De-) Democratization of Authoritarian Regimes", International studies quarterly, 2021, https://doi.org/10.1093/isq/sqab053; Pelke, L., "Inclusionary regimes, party institutionalization and redistribution under authoritarianism", Democratization 27, No. 7, 2020, https://doi.org/10.1080/13510347.2020.1786683, p. 1301–23.

[14] Huntington, S. P., "Democracy's Third Wave", Journal of Democracy 2, No. 2 1991, https://doi.org/10.1353/jod.1991.0016, p. 12–34

[15] Wu, N., Cheng, T., "Democratization as a Legitimacy Formula: The KMT and Political Change in Taiwan", New York: Palgrave Macmillan US, 2011, p. 239–60.

[16] Darmofal, D., "Demography, politics, and partisan polarization in the United States", Strickler R., (ed.), Cham, Switzerland: Springer, 2019, p. 1828–2016; Sorensen, R. J., "Political competition, party polarization, and government performance", Public choice 161, no. 3/4, 2014, https://doi.org/10.1007/s11127-014-0168-0, p. 427–50.

[17] Huang, M. H., "Polarized Politics, Government Legitimacy, and Democratic Legitimacy in Taiwan", Cambridge University Press, 2016, p. 166–89.

[18] Miller, A. H., "Rejoinder to "Comment" by Jack Citrin: Political Discontent or Ritualism?", The American political science review Vol. 68, No. 3, 1974, https://doi.org/10.2307/1959142, p. 989–1001

[19] Macdonald, D., "Political Trust and Support for Immigration in the American Mass Public", British journal of political science Vol. 51, No. 4, 2021, https://doi.org/10.1017/S0007123419000668, p. 1402–20.

[20] Uslaner, E. M., "The Oxford handbook of social and political trust", Handbook of social and political trust, New York, NY: Oxford University Press, 2018.

[21] Easton, D., "A framework for political analysis", Englewood Cliffs, N. J.: Prentice-Hall, 1965.

[22] Hetherington, M. J., "The Political Relevance of Political Trust," The American political science review Vol. 92, No. 4, 1998, https://doi.org/10.2307/2586304, p. 791–808.

[23] Miller, "Rejoinder to "Comment" by Jack Citrin: Political Discontent or Ritualism?."; Hetherington, "The Political Relevance of Political Trust."

[24] Macdonald, D., "Political Trust and Support for Immigration in the American Mass Public", British journal of political science Vol. 51, No. 4, 2021, https://doi.org/10.1017/S0007123419000668, p. 1402–20.

[25] Friedberg, E., "Conflict of interest from the perspective of the sociology of organised action", Cambridge University Press, 2012, p. 39–53.

[26] Fairbrother, M., "When Will People Pay to Pollute? Environmental Taxes, Political Trust and Experimental Evidence from Britain", British journal of political science Vol. 49, No. 2, 2019, https://doi.org/10.1017/S0007123416000727, p. 661–82.

[27] Macdonald, D., "Political Trust and Support for Immigration in the American Mass Public", British journal of political science Vol. 51, No. 4, 2021, https://doi.org/10.1017/S0007123419000668, p. 1402–20.

[28] Despite the fact that we observed such high correlation between the position of political parties and that of their supporters, this empirical observation does not tell us the causation—whether it is parties' opinions affect their supporters or the other way around.

[29] Huang, M.H., "Polarized Politics, Government Legitimacy, and Democratic Legitimacy in Taiwan", Cambridge University Press, 2016, p. 166–89.

[30] "Taiwanese / Chinese Identity(1992/06~2021/06)", Election Study Center, National Chengchi University, 20.07.2021, https://esc.nccu.edu.tw/PageDoc/Detail?fid=7800&id=6961.

# ENERGY AND CRITICAL INFRASTRUCTURE SECURITY

# ENERGY AND CRITICAL INFRASTRUCTURE SECURITY: THE CASE OF THE BALTIC STATES

IVO JUURVEE
Head of Security & Resilience Programme and Research Fellow
at the International Centre For Defence and Security

The protection of critical infrastructure in the Baltic states – Estonia, Latvia and Lithuania – has been in constant change during the last decades, and it will continue to be so in the future. It has been influenced by both internal and external developments, as well as perceived threats. There are many differences in approach among the three. However, on the other hand, all three countries are members of the European Union and NATO, and these organizations regulate many state aspects, including the functioning of the critical infrastructure.

There is no joint definition of critical infrastructure, still, in the Baltic case, electricity is a key field of critical infrastructure, as it influences all fields of human activity. On top of that, information technology is becoming almost as important as electricity in a modern state. Also, the international transport connections – including railway – are of paramount importance in the current globalizing world. Hybrid warfare might be an even more complex phenomenon to define, but there seems to be a consensus among analysts that Russian state-backed cyberattacks against Estonia in 2007[1], Belarus state-backed intrusions of immigrants into Lithuania, and forced landing of the jetliner on its way to Vilnius in 2021[2] are examples of that phenomenon. The objects of the cyberattacks – government, media and banking websites, as well as international flight as a segment of international transport – are surely part of critical infrastructure. The states' border facilities are usually considered to be ones as well, therefore, it would be fair to state that the Baltic states have some knowledge in countering previously unknown hybrid threats to critical infrastructure.

## INFRASTRUCTURE AND ITS PROTECTION

After the collapse of the Soviet Union and the regaining of independence, the Baltic states inherited an infrastructure not always suitable for their future needs. Although the Baltic states might look similar on the map, some natural differences have influenced electricity production. In the central part of Latvia, the Daugava river flows, offering possibilities of producing hydro energy in large quantities, especially at Pļaviņas Hydroelectric Power Plant and Riga Hydroelectric Power Plant – the only such river in the three states. While hydroelectric power is considered environmentally friendly, the peculiarities of electricity production in the other two Baltic states have faced major transformations due to changes in the understanding of fighting climate change. Estonia possesses large reserves of oil shale, especially in the North-East of the country, where three thermal power plants – Baltic, Estonian and Auvere, the most recent one – are situated. Lithuania is the only Baltic state that has ever produced nuclear power. It was done at the Ignalina Nuclear Power Plant, the first unit of which was operational during 1983-2004, and the second during 1987–2009.[3]

Initiatives to reduce the carbon footprint have influenced the energy sector in the Baltic states and reduced their independence. The changes have been rather fast, especially in Estonia, a country that traditionally had been exporting electricity. Estonia lost such status in 2019, and by 2020 only 55.3 % of electricity consumption was produced locally. In total, the Baltic states imported over a third of their electricity in 2020.[4]

In addition to importing electric power, there is one more form of dependency. The power grids of the Baltic states are at the moment synchronized with their Eastern neighbours via a system known as "BRELL" – the power supply system of "Belarus–Russia–Estonia–Latvia–Lithuania". Although the dependency has been to some extent mutual –

especially concerning Russia's enclave of Kaliningrad Oblast on the shores of the Baltic Sea – it has been seen as a challenge for energy security in the Baltic states. Russia has made investments to enable the possibility of desynchronizing Kaliningrad from the Baltic states, making them vulnerable. Having in mind Russia's history of weaponizing energy supply for political aims, the desynchronization of Baltic states from IPS/UPS[5] has been on the agenda for a while. The target date for Baltic transmission system operators (TSOs) to link with TSOs of continental Europe – 2025 – was finally set in 2019.[6]

Other infrastructure inherited from the Soviet Union has also been completely renovated. There is still one reminder of the occupation with the railway network still relying on the Russian gauge standard (1520 or 1524 mm) instead of the European gauge (1435 mm). Although the gauge between the port facilities of the Baltic states and Russia and Belarus will remain the same, the new fast connection to Warsaw – Rail Baltica – will use a European gauge and take the rail connection to a completely new level. According to current plans, the new line ending in Tallinn should be finished by 2026.[7] Although major construction projects tend to be delayed, the construction is well in progress.

The systems of critical infrastructure protection of the Baltic states have some similarities, but also some important differences. While it is a task of the Government in all counties, the lead ministries are different. In Estonia it is an obligation of the Government office[8], in Latvia, it falls more under the domain of the Ministry of the Interior[9], and in Lithuania under the Ministry of Defence.[10]

In all three countries, various other ministries, state agencies and service providers are involved, security services have their role and agencies also exist that deal especially with cybersecurity.[11] To test the critical infrastructure protection, different exercises are conducted, the most known of them being the cyber defence exercise Locked Shields, organized by the NATO Cooperative Cyber Defence Centre of Excellence annually since 2010, unique on the global scale.[12]

## THREATS AND DANGERS

There are mainly three kinds of threats to critical infrastructure – emanating from nature, technology failures (usually mixed human error), or hostile action. All these have shaped the understanding of the public, as seen from the discussions in the press, and mainly the last one is reflected in strategy documents in the Baltic states.

With the highest peak of only 318 m over sea level, the Baltic states are flat. The countries are not situated in a seismically active region, neither are they threatened by tsunamis or tornados. However, there are still some natural hazards to critical infrastructure and power supply, mostly caused by the cold or stormy Northern European weather. While floods are usually not dangerous and at some places even considered to be a tourist attraction (Pamarys region in Lithuania and Soomaa in Estonia), the autumn and winter storms can be more dangerous, especially in Estonia. While short term power cuts and the inaccessibility of roads are usual and appear every year with both the authorities and population well prepared for them, from time to time things get more extreme. In December 2010, almost 600 people were stuck in their cars in the snowstorm on Tallinn–Narva road. One of the main roads of the country was blocked for a day and it was a close call that nobody froze to death. Rough weather in Southern Estonia in December 2019 disrupted the power supply of over 50 000 clients and took days to fix. However, although events like these do happen in the Baltic states, they do not have disastrous effects on infrastructure.[13]

The COVID-19 pandemic has brought different kinds of problems, although also emanating from nature. The closure of some borders, especially at the beginning of the pandemic in spring 2020, showed the international transport connections – and therefore vital supplies – of the Baltic states may be at risk. Secondly, the pandemic revealed that compulsory self-isolation of persons having been in contact with an infected person might lead to unexpected consequences in companies providing vital services, since many jobs needed to keep the critical infrastructure maintained and smoothy functioning cannot be run from a distance.

Technological accidents (except the sinking of m/s Estonia caused by technology failure and extreme weather conditions in 1994, which was a part of international transport connecting Tallinn to Stockholm) have not seriously influenced the critical infrastructure, however, all countries are situated within the range between 500 to 1000 kilometres from the Chernobyl Nuclear Power Plant, the place of the humankind's worst technological disaster back in 1986. It has held the threat perception high, especially in Lithuania, even more so since Belarus has built the Astravec Nuclear Power Plant just on the other side of the border, only some 40 kilometres away from the capital Vilnius.[14]

Most threats, both to security in general and critical infrastructure in particular, are perceived to originate from hostile intent. Although the New York attacks of 2001 were noticed and taken into consideration in the Baltics,[15] there have been no serious incidents defined as terrorist attacks (although bomb explosions, usually with criminal motives, were rather common in the 1990s). Still, there have been acts of Islamist terrorism in Northern Europe.

Other hybrid threats are more plausible. Russia's aggression against Georgia in 2008 and Ukraine since 2014 have made these threats perceptible for both the decision-makers and the public. However, the Baltic states have some experience in materialising hybrid threats. In 2007, Estonia was under diplomatic, economic and informational pressure from Russia, which also applied its secret services and proxies, leading to riots in Tallinn in late April. These activities climaxed with the wide spectrum of cyberattacks against targets in Estonia – the first such occurrence becoming more common in the following years.[16] Lithuania – and to a lesser extent Latvia –were hit by Belarus deliberately directing migrant flow to their borders, also accompanied by a massive information campaign, in 2021.[17] At the time this article is written it cannot be stated that the crisis is over.

There have been some concerns lately over security aspects of the People's Republic of China (PRC) foreign investments into critical infrastructure. The concerns have involved 5G technology, but also the transport infrastructure. There was an initiative to build a railway tunnel using PRC investments, technology and labour between Tallinn and Helsinki as an extension of the Rail Baltica line, and therefore of importance to all Baltic states. However, it was turned down by the Finnish and Estonian governments in April 2021, after finding the offer suspicious. If the implementation of the tunnel idea continues, it will be handled in cooperation between the abovementioned governments.[18]

## RECOMMENDATIONS

The need for securing the critical infrastructure has been well acknowledged in the Baltic states and has been progressing, however, no system is perfect.

While planning and implementing measures to secure the critical infrastructure, the whole spectrum of natural and technological threats must be kept in mind. Last not least, threats originating from hostile action from state and non-state actors – hybrid threats – are to be considered. Due to their geographical location, natural disasters have a low probability in the Baltic states, on the other hand, the same location causes a rather high probability of hybrid threats.

The most critical infrastructure systems for modern societies are power supply and IT systems, their security is paramount to keep everything else running. Securing their continuity of operation and resilience against foreign influence by politically manipulated restrictions on supply, cyber and physical attacks is crucial.

To secure the resilience of vital services, smooth coordination between different countries, state agencies and private critical service providers is needed. Of course, it must be regulated and planned, but to be sure, it works, and overcoming the bottlenecks not foreseen by regulators and planning the exercises regularly is also of utmost importance. These should involve – not necessarily at the same time – all levels from the decision-makers in the governments to the first responders on the field or, for cyberspace, behind the screen.

The direction of lessening the dependence on the Eastern neighbours and promoting integration with the Northern and Western ones instead has been a central policy for the Baltic states since regaining independence in 1991. In the field of critical infrastructure protection, a lot has been done here –standard implementation, synchronization of regulation with EU and NATO, investment into power grid links, cooperation in different fields of security, etc. However, there is still a lot to do and multinational projects like Rail Baltica and the desynchronization from the BRELL ring serve as flagship projects, contributing not only to more resilient infrastructure but also to the security of the region as a whole.

In addition to learning from one's own mistakes, international cooperation can contribute to a better understanding of rapidly changing hybrid threats and add them to exercise scenarios and contingency planning. Although there is close cooperation inside the EU and NATO in these fields, the lesson to be learned from the other parts of the world should not be underestimated. With PRC's growing potential and willingness to project its influence also in the Baltic region, the experiences gained outside EU or NATO that have not been considered as much as they should be at the moment may be the most useful.

Although rather small, the Baltic states have some first-hand experience tackling hybrid threats that had not been tackled by democratic countries earlier or not at all, namely the Estonian experience with cyberattacks originating from Russia in 2007 and Lithuanian and Latvian experience with immigrants sent in from Belarus in 2021. Although both these dangers were rather unexpected, the answer has been efficient. Therefore, the Baltic states should not see themselves only as learners in this field but also as providers of know-how in Europe and worldwide. The Baltic cyber expertise has already benefitted democratic countries across the globe, and the same work should continue with border incidents.

## ENDNOTES

[1] Tikk, E., Kaska, K., Vihul, L., "International Cyber Incidents: Legal Considerations", Cooperative Cyber Defence Centre of Excellence, 2010, https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf, p. 18–24.

[2] Wood, G., "The Ryanair Hijacking Pierced the Delusion of Flight", The Atlantic, 28.05.2021, https://www.theatlantic.com/ideas/archive/2021/05/belarus-ryanair-hijacking/619028/.

[3] "History", Ignalina Nuclear Power Plant, https://www.iae.lt/en/about-us/history/137.

[4] Hamburg, A., “Meie savijalgadel energiamajandus”, [Our energy management on the clay feert] Postimees, 23.12.2021, https://arvamus.postimees.ee/7414387/arvi-hamburg-meie-savijalgadel-energiamajandus?utm_source=facebook.com&utm_medium=social&utm_campaign=share-buttons&utm_content=7414387&fbclid=IwAR0FVBpoWZgx7eJ28oOXESN1Io01dS5zKzBkALLGvVzeK06IqcJekqLpDFA.

[5] UOS/PSS area synchronous transmission grid consists of UPS - Unified Power System of Russia and IPS – Integrated Power System (includes Ukraine, Kazakhstan, Kyrgyzstan, Belarus, Azerbaijan, Tajikistan, Georgia, Moldova and Mongolia).

[6] “Snchronisation with continental Europe”, Elering, https://elering.ee/en/synchronization-continental-europe.

[7] “Project Timeline”, Rail Baltica, https://www.railbaltica.org/about-rail-baltica/project-timeline/.

[8] See amendments to the Article 12 of the Emergency Act of 18.06.2021, https://www.riigiteataja.ee/akt/118062021001.

[9] Djatkoviča E., Andžāns, M., “Latvia: entangled system-in-progress amidst terrorism, Russia and cyberthreats”, in Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication, Andžāns, M., Sprūds, A., Sverdrup, U., (eds.), Latvian Institute of International Affairs, 2021, https://liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1, p. 39–49.

[10] Vilpišauskas, R., “Lithuania: regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences”, in Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication, Andžāns, M., Sprūds, A., Sverdrup, U., (eds.), Latvian Institute of International Affairs, 2021, https://liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1, p. 59–87.

[11] For detailed overview of the system and regulatory framework in all three Baltic countries, see: Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication, Andžāns, M., Sprūds, A., Sverdrup, U., (eds.), Latvian Institute of International Affairs, 2021, https://liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1, p. 59–87.

[12] “Locked Shields”, CCDCOE, https://ccdcoe.org/exercises/locked-shields/.

[13] Juurvee I., Loik, R., “Estonia: building resilience through vital service providers”, Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication, Andžāns, M., Sprūds, A., Sverdrup, U., (eds.), Latvian Institute of International Affairs, 2021, https://liia.lv/en/publications/

critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1, p. 14–16.

[14] Luxmoore, M., "Lithuania fears Belarus hasn't 'learned lessons of Chernobyl'", LRT, 19.01.2020, https://www.lrt.lt/en/news-in-english/19/1133741/lithuania-fears-belarus-hasn-t-learned-lessons-of-chernobyl.

[15] Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication, Andžāns, M., Sprūds, A., Sverdrup, U., (eds.), Latvian Institute of International Affairs, 2021, p. 16, 40, 99.

[16] Juurvee, I., Mattiisen, M., "The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict", ICDS Report. August 2020, https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

[17] Adams, P., "How Belarus is helping 'tourists' break into the EU", BBC News, 22.10.2021, https://www.bbc.com/news/world-58952867.

[18] "Memorandum: Rail Baltic a precondition for Tallinn-Helsinki tunnel", ERR News, 27.04.2021, https://news.err.ee/1608192223/memorandum-rail-baltic-a-precondition-for-tallinn-helsinki-tunnel.

# ENERGY AND CRITICAL INFRASTRUCTURE SECURITY: THE CASE OF TAIWAN

CHIA-YI LEE
Associate Professor at the National Chengchi University, Taipei

This article focuses on energy and critical infrastructure security in Taiwan; *it* also analyses the challenges and opportunities Taiwan is facing. According to the U.S. Department of Homeland Security, critical infrastructure "includes the vast network of highways, connecting bridges and tunnels, railways, utilities and buildings necessary to maintain normalcy in daily life. Transportation, commerce, clean water and electricity all rely on these vital systems."[1] As the definition suggests, infrastructure (such as electricity and utilities) is included as part of critical infrastructure, along with other essential forms of infrastructure such as transportation systems and public health. Therefore, energy and critical infrastructure security mean the protection and support of these important facilities and systems. This article first reviews the developments of Taiwan's energy and critical infrastructure. Then it discusses the main challenges for Taiwan's energy and critical infrastructure security. The article concludes with lessons drawn and provides recommendations for future policies surrounding these issues.

## BACKGROUND OF ENERGY AND CRITICAL INFRASTRUCTURE DEVELOPMENTS IN TAIWAN

This section reviews the history of Taiwan's energy and critical infrastructure developments. It discusses three periods – the period of Japanese colonial rule (1895-1945), the period of Kuomintang (KMT) authoritarian rule

(1945–1996), and the period after Taiwan's democratization (1996–present). Exploring those issues will provide an understanding of the developments of Taiwan's energy and critical infrastructure.

## JAPANESE COLONIAL RULE (1895–1945)

The developments of Taiwan's critical infrastructure can be traced back to the 50 years of Japanese colonization starting in the late 19th century. Japan as a colonizer mainly did three things to develop the critical infrastructure in Taiwan. First, it improved Taiwan's public health conditions, e.g., by building hospitals and promoting island-wide vaccinations. Second, Japan developed the essential transport infrastructure. This included building the post system, constructing the north-south railway, and opening ports. Finally, it included building the energy system, such as constructing Taiwan's first hydropower plant in 1905 and establishing the Taiwan Electricity Corporation (today's the Taiwan Power Company) in 1919. The first steps for Taiwan's modernization occurred with these developments and other constructions, such as the building of water and land systems.

## KMT AUTHORITARIAN RULE (1945–1996)

Taiwan's economy experienced several years of post-war recessions after World War II and the beginning of KMT rule. To transform Taiwan's economy from an agriculture-based one to an industrial one, the KMT government first promoted import substitution and later export-oriented industrialization in the 1950s and 1960s. In the 1970s, after the global oil crisis, the government launched the Ten Major Construction Projects, which included six transportation projects, three heavy industrial projects, and one energy project. The Ten Major Construction Projects built a solid foundation for Taiwan's fast economic growth in the 1980s, and partly helped Taiwan become one of the Four Asian Tigers.

In 1984 and 1990, the government subsequently launched the Fourteen Construction Projects and the National Construction Six Years Project, both focusing on critical infrastructure such as highways, railways, power plants, public health, and medical insurance. Taiwan became one of the top 20 economies (in terms of GDP) in the world in 1993. This was the so-called "Taiwan Economic Miracle" period, when both the economy and the development of critical infrastructure were fast growing in Taiwan. This history suggests that building critical infrastructure is key to a country's economic development.[2]

### THE POST-DEMOCRATIZATION PERIOD (1996–PRESENT)

In 1996, Taiwan had the first direct presidential election – a milestone marking Taiwan's democratization by the Western standard. In 2000, Taiwan witnessed party alternation for the first time, with the Democratic Progressive Party (DPP) replacing the KMT and becoming the ruling party. However, Taiwan's economic growth slowed down in the 2000s, and the stagnant economic growth lasted for almost 20 years until recent times. Despite the economic slowdown, during this period, Taiwan's economy has reduced dependence on manufacturing and moved towards a high-tech society. The developments of modern infrastructure such as the Mass Rapid Transit (MRT), the high-speed railway, the internet, and renewable energy projects were also launched during this period. This period can be seen as a stabilizing transformation period considering Taiwan was no longer pursuing fast economic growth and the government was paying more attention to the public's well-being.

## PRIMARY CHALLENGES OF ENERGY AND CRITICAL INFRASTRUCTURE SECURITY IN TAIWAN

The above section suggests that the developments of energy and critical infrastructure in Taiwan have been quite stable and smooth, despite various challenges. This section analyses the challenges of energy and critical infrastructure security in Taiwan, focusing on three issues: transportation, energy security, and cybersecurity. The transport sector is essential to a country's economy and people's daily life. Energy is also crucial to the economy, people's livelihood, and to national security. Cybersecurity is a relatively new issue emerging in the digital era which may impact society in a significant way. Thus, it is important to understand what challenges Taiwan is facing regarding these three issues.

## CHALLENGES TO TRANSPORTATION

Taiwan's public transportation is relatively efficient and convenient, but it faces three primary challenges: urban-rural disparity, poor traffic design, and high carbon emissions. It is easy to travel around without one's vehicle, thanks to the MRT system and the dense bus network in big cities like Taipei. Residents face a certain level of difficulty travelling from their homes to elsewhere in some rural or mountainous areas, however. The traffic design in Taiwan can be improved as well. Taiwan's road traffic safety has long been criticized despite Taiwan being hailed as one of the safest places in the world. In addition to many drivers' lack of good driving habits, which often cause traffic jams or accidents, one more reason for the criticism is poor traffic design. For example, many streets are not designed to prioritize pedestrians or cyclists, which increases their vulnerability. The transportation sector has also been a strong contributor to Taiwan's greenhouse gases emissions over the past few decades. From 1990 to 2019, the percentage of carbon dioxide emissions from the transport sector has only dropped from 18% to 14%, making it the third-largest emitter after the energy sector and the industrial sector.

Taiwan's transportation sector is vulnerable to external threats as well in addition to the previously noted domestic challenges. Taiwan is an island that is highly reliant on maritime and air transport, through which essential and vital resources such as petroleum are supplied from overseas. Taiwan has only four major international ports (Keeling, Taichung, Kaohsiung, and Hualien) and one major international airport (Taoyuan International Airport) despite having a population of 23 million. This suggests that a blockade of these key transport facilities may deeply hurt Taiwan's survival, making Taiwan a helpless and isolated island in a war. Even without a military blockade, the fact that many transport facilities are computer-controlled nowadays means that the transportation sector is vulnerable to cyberattacks or other forms of hybrid threats.[3] So the protection of these air, maritime, and land transport installations is very important.

## CHALLENGES TO ENERGY SECURITY

Energy security is defined as a "reliable and adequate supply of energy at reasonable prices".[4] It has always been a major concern for advanced economies, especially those not domestically producing energy. Taiwan also faces an energy insecurity issue considering it is an island country – and is heavily dependent on sea-based energy imports. There are three primary challenges.

First, because Taiwan imports almost all the energy it consumes from abroad, predominantly by maritime transportation, risk of supply disruptions exists. For example, Taiwan mainly purchases crude oil from the Persian Gulf countries such as Saudi Arabia and Kuwait. The crude oil Taiwan imports is shipped by seaborn routes through the South China Sea. The Middle East's instability and the South China Sea's vulnerability to military blockade both pose a threat to Taiwan's energy supply stability.

Second, Taiwan's energy prices are subject to the global market fluctuations considering its reliance on overseas energy resources. The gasoline and electricity prices in Taiwan are relatively cheap and less volatile compared to other advanced economies in the world. This, however, is due to the fact that the major petroleum company and electricity companies in Taiwan – the China Petroleum Corporation Taiwan (CPC) and the Taiwan Power Company – are state-owned enterprises that do not run for profits. In other words, it is government subsidies that keep energy prices low and stable. Although Taiwan's fuel market has already been liberalized, currently it is still monopolized by two companies (CPC and Formosa Oil). Many also argue that the government should open the electricity market.[5] End-users may expect to pay the market prices, which could be higher and more unstable than the current prices if Taiwan's energy market is fully liberalized. This is especially the case if the feed-in tariff that is adopted to promote renewable energy is taken into account.[6]

Third, Taiwan's electricity demand has kept rising. This is partly due to, first, the large power consumption in the electronics industry; second, to climate change and, third, to high demand for air-conditioning during the summer months. So, the short-term supply of electricity sometimes cannot meet the peak demand. It is an issue manifested by the occasional power outages in Taiwan in recent years. Part of the reason for these problems is the DPP government pushing for energy transitions to change Taiwan's energy system from being reliant on fossil fuels (especially coal which has been the most polluting) to low-carbon sources. The DPP government also plans to phase out nuclear power by 2025. The shortage in electricity due to reductions in coal-fired power and nuclear power is expected to be met by increasing usage of renewable energy and liquefied natural gas (LNG).

Energy transitions are necessary and have become a global trend as a significant effort to combat climate change. Like in some other countries in the world, however, energy transition policies have also aroused a great deal of controversy in Taiwan. One reason is that nuclear power has been a political issue in Taiwan for decades. It's an issue that divides the DPP and KMT. The former mainly opposes nuclear power, while the latter supports it. Many accuse the DPP government of abolishing nuclear power based on political ideology and ignoring the fact that nuclear power is more stable, can generate electricity more efficiently, and emit less carbon dioxide. Other energy policies implemented by the DPP government, including building offshore wind farms and a plan to build a new LNG terminal in Taoyuan, have also faced strong opposition from local environmentalists and anti-DPP activists.[7] It will be more difficult for Taiwan to achieve a smooth energy transition when energy issues are politicized.

## CHALLENGES TO DIGITALIZATION AND CYBERSECURITY

The final challenge this section discusses is a dilemma Taiwan is facing in the digital era. On the one hand, Taiwan's digitalization can be improved, which will enhance efficiency and reduce waste. On the other hand, increasing dependence on cyberspace may pose a challenge to cybersecurity. The level of digitalization in Taiwan is relatively low compared to other developed countries, despite a broad dependency on high tech industries. This is especially the case in the public sector and among small businesses, probably due to Taiwan's high wealth inequality.[8] Government officials and civil servants often spend time in inefficient paperwork and red tape. Digitalization has been accelerated in recent years. This is partly due to the government promoted Digital Government Program; but also is the result of the COVID-19 pandemic, which prevents people from closely contacting one another. There is still room for improvement despite Taiwan's existing efforts at digitalization.

Indeed, digitalization enhances government efficiency and reduces waste of resources, but it also creates a potential cybersecurity threat. There are a variety of definitions for cyber security. Von Solms and Van Niekerk argue that it "is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace."[9] Cybersecurity is consequently a broad concept that covers the protection of information and any assets related to cyberspace such as information and communication technology.

In the digital era, cybersecurity becomes a critical issue for countries that highly rely on cyberspace, automation, and computerization to function, and Taiwan is no exception. The Taiwanese government has invested in the government cloud infrastructure, but this pursuit also makes the government data or computer systems vulnerable to cyberattacks or even cyberterrorism. Cyberterrorism is "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)."[10] Although so far cyberattacks on Taiwan's government agencies or private companies have been carried out by hackers who simply demand money, the threat of cyberattacks to national security cannot be underestimated.

One of the cybersecurity problems that is particularly pertinent to Taiwan is information warfare. Information warfare entails manipulating, exploiting, or denying information received by the target; it can be launched more effectively in the digital era through social media. Experts believe China has waged information warfare against Taiwan, including via spreading disinformation.[11] Increasing reliance on the internet will worsen the problem – many Taiwanese who have access to the internet may be influenced by the propaganda from China. Tightening control of the internet or social media, however, is not a good solution, as it will intrude into the freedom of speech which is highly valued in democratic Taiwan. So how to strike a balance between internet freedom and the fight against information warfare is an important issue for the government.

## RECOMMENDATIONS FOR FUTURE POLICIES

After discussing the challenges to energy and critical infrastructure security in Taiwan, this section offers a list of recommendations for further policy developments. Three areas are covered: the transport sector, energy security, and cyber security.

First, the government should make a greater effort to improve traffic design and public transportation, especially in rural areas. To prevent the transportation sector from being vulnerable to hybrid threats, the government should also enhance the security and resilience of key transport facilities. The recommendation can be pursued for example by improving the information system and strengthening the physical protection of the airports and ports. The government should also inform the public of potential threats. The suggested effort will increase their awareness and alert as a result.

Second, energy security is important to Taiwan's economy, national defence, and people's daily life. The government should strengthen efforts in enhancing Taiwan's energy security while simultaneously promoting a smooth energy transition. The ongoing energy transition policies should not be abandoned, despite the opposition, but can be adjusted from time to time. For example, the government can consider slowing down the pace of nuclear phaseouts when the construction of offshore wind farms or other renewable energy projects is not on time. Moreover, the government should ensure that the energy system is firmly protected and the energy supplies are reliable and diversified. Taiwan's energy security is vulnerable to any attempt that could disrupt the energy provision given its status as a major energy importer. Avoiding the over-dependence on a single source or only a few sources is important.

Lastly, cybersecurity and the related issues of disinformation, fake news, and information warfare pose a significant threat to Taiwan. The threat may loom in the future as Taiwan accelerates digitalization. The government needs to protect cyberspace, information systems, and technology but at the same time, everyone's freedom in cyberspace must be ensured. This requires the government to make laws or policies that can effectively manage cybersecurity while not intruding into civil liberties. The problem is that technological innovation is sometimes too fast for government regulations or legislation to catch up. Consequently, the government has to review and update these policies or regulations very often. The current President of Taiwan Tsai Ing-Wen recently announced a plan to establish the Cybersecurity Administration. It will integrate different government agencies focusing on information and digital issues. This represents an important step towards raising cybersecurity to the level of national security – a level vital to Taiwan's prosperity and stability in the digital era.

In sum, while Taiwan has a well-developed and improving critical infrastructure, including in the transportation sector and the energy sector, the security risk to these systems cannot be underestimated. The increasing reliance on the internet and the computerized control of these critical facilities pose challenges to Taiwan's energy and critical infrastructure security. It renders them vulnerable to cyberattacks or other forms of manipulation. The risk is also higher considering Taiwan's dependence on imports owing to its standing as an island country. This is an issue that the government and the public should be aware of and make efforts to address.

## ENDNOTES

[1] "Critical Infrastructure", Homeland Security. Accessed on October 14, 2021, https://www.dhs.gov/science-and-technology/critical-infrastructure. This article uses this definition and will focus on energy, transportation, and other critical infrastructure. However, because energy is critically important to a country's economy as well as national defence, this article pays special attention to energy and sometimes separates the discussion of energy from other critical infrastructure.

[2] Reinfeld, W., "Tying infrastructure to economic development: The Republic of Korea and Taiwan (China)", Infrastructure strategies in East Asia: The Untold Story, p. 3–26, 1997.

[3] Hybrid threats differ from conventional warfare in that they are "the simultaneous employment of the range of possible instruments, from threats of war to propaganda and everything in between" by an adversary in order to achieve the same outcome without actual war. See Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., McCue, M., "Addressing Hybrid Threats", Center for Asymmetric Threat Studies, The European Centre of Excellence for Countering Hybrid Threats, Swedish Defence University, 2018.

[4] Bielecki, J., "Energy security: is the wolf at the door?", The Quarterly Review of Economics and Finance 42 (2), 2002, p. 235-250.

[5] For example, see Hsu, C., "Taiwan should liberalize energy market: chamber", Taipei Times, 06.11.2019, https://www.taipeitimes.com/News/biz/archives/2019/11/06/2003725308.; Yang, C.H., Wang, C., "The Energy Regulation and Markets Review: Taiwan", 16.06.2021, https://thelawreviews.co.uk/title/the-energy-regulation-and-markets-review/taiwan.

[6] Sheng, T., Po-Han, C., "A dual market structure design for the reform of an independent power grid system—The case of Taiwan", Energy Reports Vol 5, 2019, p. 1603–1615.

[7] Suspicions exist that these opposition groups might be supported or incited by the Chinese government as a way to increase frictions in the Taiwan society, but so far, no clear evidence has indicated this is true.

[8] Ngerng, R., "To Step up Its Digital Transformation, Taiwan Needs a New Social Compact", The Diplomat, 05.12.2020, https://thediplomat.com/2020/12/to-step-up-its-digital-transformation-taiwan-needs-a-new-social-compact/.

[9] Solms, R., Niekerk, J., "From information security to cyber security", Computers & Security Vol. 38, 2013, p. 97–102.

[10] Weimann, G., "Cyberterrorism: The sum of all fears?", Studies in Conflict & Terrorism Vol. 28(2), 2005, p. 129–149. The definition suggests that if a country is more reliant on computer networks or internet to operate important facilities, this country is more vulnerable to cyberterrorism.

[11] Su-wei, W., Tu, A., Xie, D., "Experts warn over information warfare from China", Taipei Times, 14.07.2020. Accessed on October 21, 2021, https://www.taipeitimes.com/News/taiwan/archives/2020/07/14/2003739897.

# CYBERSECURITY

# CYBERSECURITY AND HYBRID THREATS IN THE DIGITAL BALTIC STATES: A STATE OF THE ART

**LOUIS WIERENGA**
Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu I
Lecturer in International Relations, Department of Political and Strategic Studies,
Baltic Defence College

In a very recent and insightful study on AI for digital warfare, Hageback and Hedblom (2022) in their synonymous monograph pose a fascinating question: what Clausewitz would have thought of digital warfare.[1] Hageback and Hedblom (2022) then correctly note that the new digital technology which we are now in possession of has led way to a new digital sphere which substantially increases the speed, reach, stealth, precision, diffusion, and breadth of a potential attack.[2] Much has changed in the realm of cybersecurity and cyberwar since academic literature first took note.

There is broad consensus amongst academics and policy makers that the nature of warfare and security is changing.[3] While this is not disputed, and warfare changes and progresses with time, this claim should be placed within the broader notion of a changing geopolitical landscape and a multipolar world order and in light of Hageback and Hedblom's (2022) aforementioned observation, relating to digital warfare and cyber conflict. Moreover, there is a growing consensus that within renewed great power competition, the likelihood of a 'great power war' is enough to resurrect old fears and direct contemporary security debates. Hybrid warfare usually precedes kinetic warfare or take place simultaneously.[4] The targets of acts of hybrid aggression tend to be small states which are geographically near greater powers which seek to dominate them.[5]

Thus, this article focuses on cybersecurity and hybrid threats facing the three Baltic states, collectively known as Estonia, Latvia, and Lithuania.

First, I provide a brief overview of the development of cyber security and hybrid threats in the region, and a brief synopsis of the current state of affairs and conclude by offering some policy recommendations. Although the Baltic states are small states, they carry a big stick when it comes to dealing with cyber and hybrid threats. This can be used as an advantage not only internally when dealing with hostile actors in cyberspace, but when bolstering their voice within NATO and the EU. Estonia has been active in doing precisely this and Lithuania and Latvia are also answering the call.

## THE DEVELOPMENT OF CYBERSECURITY IN THE BALTIC STATES: PRIMARY CHALLENGES, RISKS, AND LESSONS LEARNED

Estonia, the small Baltic nation of just over 1.3 million people, certainly packs a big punch when it comes to all things digital, becoming the world's most advanced digital society. The small, digital nation suitably markets itself as 'e-Estonia', with a center bearing the name. Collectively, the three Baltic states fare very well in cyber-preparedness. All three are ranked by the Global Cybersecurity Index (GCI) in the top 20 out of 193 countries. Estonia places third, after only the United States and the United Kingdom.[6] Lithuania is ranked 6th, whereas Latvia is further down, ranking fifteenth.[7] Lithuania and Estonia rank very high in the National Cyber Security Index (NCSI), among the top ten,[8] whereas Latvia is slightly behind, placing 25th.[9]

The aforementioned rankings are both impressive and encouraging. However, an alarming ranking to be placed within is the ten counties which are most likely to experience brute-force attacks on Remote Desktop Protocol (RDP) services.[10] RDP brute-force attacks account for over 80 percent of all network accounts in each of the Baltic states.[11] Yet, the Baltic states remain vigilant.

Within the short history of the Baltic states, post-occupation, it has usually been Estonia leading the charge. However, this is not always the case. For instance, in 2019, Latvia was among the first countries in Europe to launch 5G (fifth generation) for commercial use and a year later opened the first military 5G test site in Europe, located at the Ādaži military base.[12]

Lithuania has also been incredibly proactive in facing up to cyber threats. A recent initiative in the summer of 2021 was the establishment of the Regional Cyber Defence Centre (RCDC).[13] The RCDC operates under the Lithuanian Ministry of National Defence. The RCDC relies on bilateral partnerships. Most strongly with the United States, as well as with Ukraine and Georgia.[14] The RCDC is one of two cyber defence centres in the Baltics, the other being the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

It is hard to separate technical innovation from what history has taught the Baltic states, in terms of facing larger powers with nefarious intentions and a faulty understanding of territorial integrity. Many academics and policy makers and think tankers have noted the change in the global power balance, the changing nature of warfare[15], as well as the growing importance of cyberspace as a battleground.[16]

In 2015, Richard Stiennon warns in his book which bears the candid title "*There Will be Cyberwar*" of precisely this. Stiennon ends his 2015 publication highlighting geographical hotspots of potential conflict: the loss of Taiwan, naval defeat in the South China Sea, and the loss of territory and sovereignty in Eastern Europe to Russia.[17]

If 2007 was the initial alarm bell for cyber and hybrid threats in the Baltics, 2020 and the onset of the global COVID-19 pandemic marks another notable date. Two important reasons underlie this. First, due to the lockdowns and social distancing practices enacted across most of the globe and in all Western democracies, education, higher education and a great degree of business was moved online.[18] Therefore, online platforms became 'the new normal and were utilized to a much greater extent, leading to the possibility of greater cyber threats. In the EU, major cyberattacks jumped from 146 in 2019 to 304 in 2020.[19] This is something that Welscher (2021) argues has both reshaped cyberspaces as a whole and presented new threats to the Baltic states.[20] There has been time to catch up and adjust. However, initially, due to the rapid move online, security became an afterthought in much of Europe.[21] Cybercrime increased losses on a global scale by more than 50 percent, hitting also the Baltic states.[22] This highlights the dire importance of remaining not just cyber-prepared, but one step ahead.

Second, and pertaining to hybrid and information warfare, both the increased amount of time people spend online during the ongoing pandemic as well as the ripe nature of a crisis of such magnitude for the spread of misinformation, disinformation, and conspiracy theories highlight crucial vulnerabilities. A 2021 report for the European Commission found, perhaps unsurprisingly, that the COVID-19 pandemic served as a catalyst for conspiracy theories.[23] This at a time of extreme political and social polarization, coupled with preference bubbles and echo chambers, which allow misinformation and disinformation to both travel and be accepted by a wider audience. Though, with threats also come solutions, better resilience, and the possibility for a united front and further cooperation with allies.

In light of power competition vis-à-vis cooperation with the US, NATO, and the EU, and small states standing up to larger powers with nefarious intentions, the drawback is that no entity is capable of defeating all cyberattacks; rather, in order to succeed in cyberspace, the key is learning how to adequately cope.[24] When it comes to information warfare, and one of the reasons for which it is so dangerous, is that the antagonist need not win – they succeed if they are able to successfully cloud the issue.[25] It is no secret that Russia has waged numerous information warfare campaigns in the Baltics and show no sign of giving up.

## RECOMMENDATIONS AND POLICY DEVELOPMENTS

### KEEP ON THE CUSP OF CYBER HYGIENE AND WIDELY PROMOTE AMONGST CITIZENS:

General H.R. McMaster notes the importance of American efforts to conduct reconnaissance in cyberspace and preempt attacks.[26] Strive to continuously be one step ahead of hackers. Although this is a daunting, if not (nearly) impossible task, it is one which would involve both governments and the general public. One aspect which has greatly contributed to the success of Estonia in becoming a world leader in cyber defence is investing in people.[27] Promoting cyber hygiene is one aspect at which Estonia excels. Raising further awareness about media literacy to combat disinformation and misinformation also helps to win the battle against information warfare. McMaster also advocates for the US to learn from countries which were on the receiving end of Russian aggression.[28] As one of the strengths which Estonia possesses is its investment in people, Estonia is a success story in cyber and IT education and training, ranging from kindergarteners to the elderly.[29]

In an increasingly multipolar world order, the rise of China presents a serious security challenge to Europe and the Transatlantic alliance and can be seen on a number of fronts. One of the most pressing, especially when it comes to cybersecurity, is 5G. If seen through the lens of 'the West', then a united front should consist of the US and NATO, plus PfP countries, along with the EU in cyber policy. When it comes to 5G, this is especially important. The Baltic states have taken strides to become leaders in 5G policy and can use this opportunity to take a leading role in a Western front in the battlegrounds for 5G policy.

## KEEPING FOCUS ON BOTH CHINA AND RUSSIA AS THREATS TO THE SECURITY OF NATO AND THE EU:

For valid reasons – both historical and contemporary – the Russian Federation is identified as the primary security threat to the 3 Baltic states. The most contemporary events in the neighborhood do not indicate any change in the consistency or persistence of the threat, nor its digital nature. Cyber and hybrid threats directed towards the Baltic states from the Russian Federation will not cease and military, government, and civilian entities need to continue with vigilance, adapt to the rapidly changing nature of cybersecurity and cyberwar, as well as anticipate future changes, staying ahead of the curve.

However, despite the very valid concerns over Russian cyber activity, the Baltic states should not neglect such concerns as they relate to China. Indeed, as aforementioned, the Baltic states, especially Lithuania, have taken a firm stance towards China, in cyberspace and beyond, and should continue to use their growing digital prowess to expand their influence in the EU and NATO. Lithuania, under the leadership of Foreign Minister Gabrielius

Landsbergis, has increasingly stood up to China.[30] Minister Landsbergis's stance towards China led to him being named as one of Politico's 'most influential people in Europe' – and the only one to make the list from any of the Baltic states.[31] Latvia has called upon China to respect the rules of international cyberspace.[32]

It should be noted that this is certainly not the first time that leaders from the Baltic states have appeared on similar lists, granting small states representation on lists where the usual larger powers within Europe enjoy substantial representation. Such leadership should be emulated, and the digital advances made by the Baltic states provides an ideal way to achieve this, as many countries look to the Baltics as digital leaders.

## DEMONSTRATING LEADERSHIP TO ALLIES:

If ever there was a time, as well as a concrete area for the Baltic states to showcase their strengths as small states, demonstrating leadership in the cyber and tech fields presents the perfect opportunity. Estonia has been the Baltic champion for cybersecurity and e-governance. Lithuania, and to a lesser extent Latvia have shown signs of catching up. Much like offline matters, the three Baltic states use opportunities to meet with US and EU leaders to highlight the dire security situation which the Transatlantic alliance faces from a resurgent Russia – they know from experience and contemporary matters.

As the security of cyberspace is one of the acute questions of global politics this century[33], cybersecurity and matters of digital warfare will be issues which merit pressing resolve, which is constantly changing. Being on the cutting edge will require countries to remain that way. While member of the United Nations Security Council for the first time, Estonia made cybersecurity a priority, along with the overall security of the region.[34] As well, when a member of the UN Security Council, Estonia made it a point to align with the US and the UK to call Russia out over a cyberattack directed at Georgia.[35]

Latvia and Lithuania have also been active on such fronts. In 2021, Latvia signed an agreement with Poland which establishes a framework for cooperation between Latvia's Military Information Technology Security

Incident Team (MilCERT) and Poland's National Cyber Security Center.[36] Latvia is also taking the opportunity to reach out to the United States to discuss cybersecurity in the region.[37] Lithuania has, as aforementioned, developed their own cyber center the RCDC, which is a bilateral Lithuanian-US initiative.[38]

## CONCLUSION

To conclude, the domain of cyberspace will be an arena for battle for the foreseeable future. All countries, governments, militaries will be faced with such threats, and the likelihood of businesses and private individuals being faced with such threats is high. The Baltic states are no strangers to such threats and have been leaders in facing up to them. Given the nature of threats faced and the manner in which the Baltics have faced up to them, it is safe to say that the Baltic states will continue to rise up to the challenges and keep up with the rapidly changing nature of cyber threats. However, the last point is the most persisting challenge any entity faces in cyberspace – the need to not only consistently keep up but remain steps ahead of adversaries. The bi- and multilateral agreements made as well as the leadership demonstrated, and the digital awareness can go a long way to not only meet contemporary and future challenges but serve as examples and demonstrate leadership. Cyber and hybrid threats are ominous, but on a positive note, the Baltic states have achieved many remarkable accomplishments in this field.

### ENDNOTES

[1] Hageback, N., Hedblom, D., "AI for Digital Warfare", Boca Raton, London, and New York: CRC Press, Taylor & Francis Group, 2022, p. 101.

[2] Ibid, p. 102.

[3] McFate, S., "The New Rules of War: Victory in the Age of Durable Disorder", New York: William Morrow, 2019; "How European Security is Changing", Chatham House, 10.01.2022, https://www.chathamhouse.org/2022/01/how-european-security-changing.

[4] Deibert, R., "Cyber-security", in Routledge Handbook of Security Studies, 2nd Edition, Cavelty, M.D., Balzazq T., (eds.), London and New York: Routledge Taylor & Francis Group, 2017, p. 324.; "U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault", The New York Times, 20.12.2021. Accessed January 3, 2022, https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html?searchResultPosition=4. NB: This article is citing an interview with US Senator Angus King, a member of the Senate Intelligence Committee.

[5] Hageback N., Hedblom, D., "AI for Digital Warfare", Boca Raton, London, and New York: CRC Press, Taylor & Francis Group, 2022, p. 103.

[6] Global Cyber Security Index, 2020.

[7] Ibid.

[8] "The National Cyber Security Index ranks 160 countries'cyber security status", e-Estonia.com, May 7, 2020, https://e-estonia.com/the-national-cyber-security-index-ranks-160-countries-cyber-security-status/

[9] NCSI, "Index." ncsi.ega.ee. https://www.ncsi.ega.ee/ncsi-index/?order=rank.

[10] Welscher, A., "More than a virus: pandemic and online security in the Baltic states", Eng.lsm.lv, 12.04.2021, https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/.

[11] Ibid.

[12] Rakštytė, A., "How can the Baltic States Support 5G Security through Transatlantic Cooperation?", Cepa.org, 26.04.2021, https://cepa.org/how-can-the-baltic-states-support-5g-security-through-transatlantic-cooperation/.

[13] "Regional Cyber Defence Centre Officially Starts Work", Ministry of National Defence, Republic of Lithuania,15.07.2021. Accessed December 3, 2021, http://kam.lt/en/news_1098/current_issues/regional_cyber_defence_centre_officially_starts_work.html?__cf_chl_f_tk=P8C9yUpzGKfAgD3YAAlVStKJ9YXscXNQtBCfIzHXD2M-1642453204-0-gaNycGzNBGU.

[14] "Regional Cyber Defence Centre Officially Starts Work", Ministry of National Defence, Republic of Lithuania, 15.07.2021. Accessed December 3, 2021, http://kam.lt/en/news_1098/current_issues/regional_cyber_defence_centre_officially_starts_work.html?__cf_chl_f_tk=P8C9yUpzGKfAgD3YAAlVStKJ9YXscXNQtB-CfIzHXD2M-1642453204-0-gaNycGzNBGU.

[15] Coker, C., "Future War", Cambridge: Polity, 2014; Packer J., Reeves, J., "Killer Apps: War, Media, Machine", Durham: Duke University Press, 2020; Hageback N., Hedblom, D., "AI For Digital Warfare", Boca Raton, London, and New York: CRC Press, Taylor & Francis Group, 2022; McFate, S., "The New Rules of War: Victory in the Age of Durable Disorder", New York: William Morrow, 2019; McMaster, H. R., "Battlegrounds: The Fight to Defend the Free World", New York: Harper, 2020.

[16] Watts,C., "Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News", New York: Harper; Stiennon, R., "There Will be Cyberwar: How the Move to Network-Centric War Fighting has set the Stage for

Cyberwar", Birmingham: IT-Harvest Press, 2015; Deibert, R., "Cyber-security" in Routledge Handbook of Security Studies, 2nd Edition, Cavelty, M.D., Balzazq, T., (eds.), London and New York: Routledge Taylor & Francis Group, 2017.

[17] Stiennon, R., "There Will be Cyberwar: How the Move to Network-Centric War Fighting has set the Stage for Cyberwar", Birmingham: IT-Harvest Press, 2015, p. 136.

[18] Kahl, C., Wright, T., "Aftershocks: Pandemic Politics and the End of the Old International Order", New York: St. Martin's Press, 2021, p. 230–231.

[19] Walsh, N. P.,"Serious Cyberattacks in Europe Doubled in the Past Year, New Figures Reveal, as Criminals Exploited the Pandemic", edition.cnn.com, 10.06.2021. Accessed 12 January 2022, https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html.

[20] Welscher, A., "More than a virus: pandemic and online security in the Baltic states", Eng.lsm.lv, 12.04.2021, https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/.

[21] Walsh, N.P., "Serious Cyberattacks in Europe Doubled in the Past Year, New Figures Reveal, as Criminals Exploited the Pandemic"m edition.cnn.com, 10.06.2021. Accessed 12 January 2022, https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html.

[22] Welscher, A., "More than a virus: pandemic and online security in the Baltic states", Eng.lsm.lv, 12.04.2021, https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/. For example, the parent bank of one bank which operated in Estonia, had its terminals stalled for several hours, which hindered millions of euros from proceeding in transaction.

[23] Farinelli, F., "Conspiracy theories and right-wing extremism – Insights and recommendations for P/CVE", European Commission, 2021, https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran/publications/conspiracy-theories-and-right-wing-extremism-insights-and-recommendations-pcve-2021_en.

[24] Schneider, J., "A World Without Trust: The Insidious Cyberthreat", Foreignaffairs.com, January/February 2022, https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust.

[25] Stengel, R., "Information Wars: How We Lost the Global Battle Against Disinformation & What We Can Do About It", New York: Atlantic Monthly Press, 2019, p. 107.

[26] McMaster, H. R., "Battlegrounds: The Fight to Defend the Free World", New York: Harper, 2020, p. 115.

[27] Kottasova, I., "How Russian Threats in the 2000s Turned This Country Into the Go-to Expert on Cyber Defence", Cnn.com, 18.06.2021, https://edition.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html.

[28] McMaster, H. R., "Battlegrounds: The Fight to Defend the Free World", New York: Harper, 2020, p. 116.

[29] Ibid.

[30] "Gabrielius Landsbergis The Dragonslayer", Politico, https://www.politico.eu/list/politico-28-class-of-2022-ranking/gabrielius-landsbergis/.

[31] "Politico 28 The Class of 2022", Politico, https://www.politico.eu/politico-28-class-of-2022/.

[32] "Latvia Calls on China to Stick to International Cyberspace Rules", eng.lsm.lv, 20.07.2021, https://eng.lsm.lv/article/society/crime/latvia-calls-on-china-to-stick-to-international-cyberspace-rules.a413570/.

[33] Deibert, R., "Cyber-security" in Routledge Handbook of Security Studies, 2nd Edition, Cavelty, M.D., Balzazq, T., London and New York: Routledge Taylor & Francis Group, 2017; Deibert, R., "Black Code: Surveillance, Privacy and the Dark Side of the Internet", Toronto: Random House, 2013.

[34] "Estonia in the Security Council: The First Year", Republic of Estonia, Ministry of Foreign Affairs, https://vm.ee/en/activities-objectives/estonia-united-nations/estonia-security-council-first-year.

[35] Kottasova, I., "How Russian Threats in the 2000s Turned This Country Into the Go-to Expert on Cyber Defence", CNN, 18.06.2021, https://edition.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html.

[36] "Latvia and Poland Sign Military Cyber Defence Agreement", Eng.lsm.lv, 23.11.2021. Accessed January 3, https://eng.lsm.lv/article/society/defense/latvia-and-poland-sign-military-cyber-defense-agreement.a431303/?utm_source=lsm&utm_medium=article-bottom&utm_campaign=article.

[37] "Baltic States and US Discuss Cyber Security", Eng.lsm.lv, 22.10.2021. Accessed December 3, 2021, https://eng.lsm.lv/article/society/defense/baltic-states-and-us-discuss-cyber-security.a426816/.

[38] Rakštytė, A., "How can the Baltic States Support 5G Security through Transatlantic Cooperation?", Cepa.org, 26.04.2021, https://cepa.org/how-can-the-baltic-states-support-5g-security-through-transatlantic-cooperation/.

# CYBERSECURITY IN TAIWAN: CHALLENGES AND RESPONSES

CHARLES K.S. WU

Assistant Professor, Department of Political Science and Criminal Justice,
University of South Alabama

HSUAN-YU (SHANE) LIN

Pre-doctoral Research Fellow, Fairbank Center, Harvard University;
PhD Candidate, Department of Politics, University of Virginia

YAO-YUAN YEH

Chair and Associate Professor, Department of International Studies
& Modern Languages, University of St. Thomas, Houston

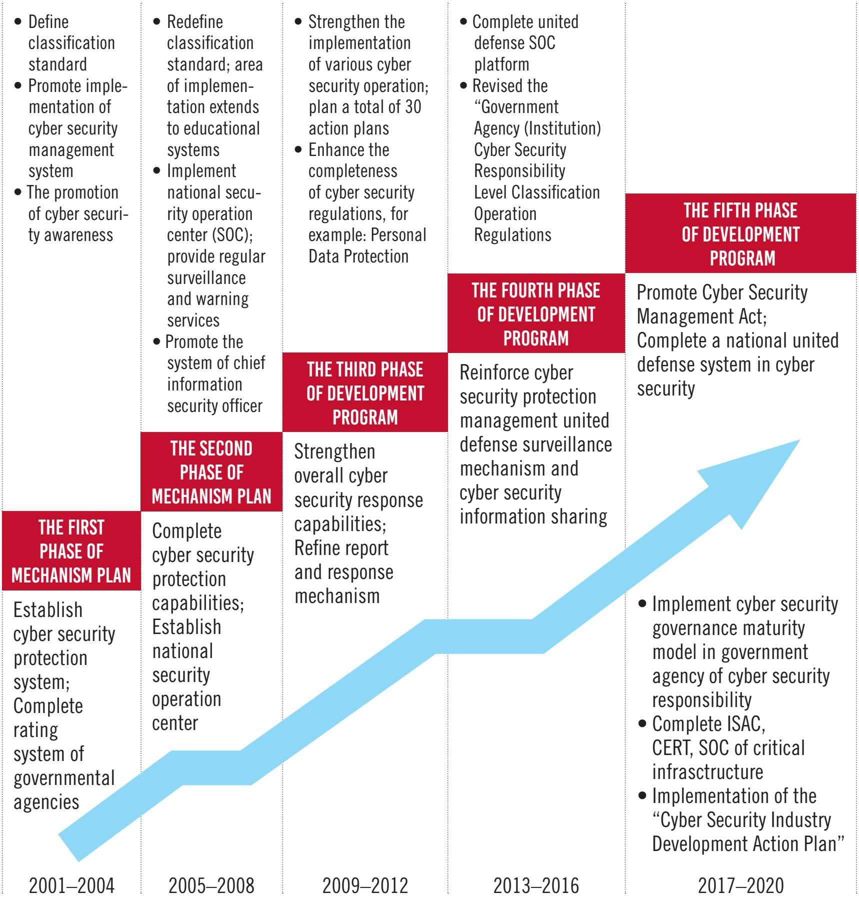
A future war between Taiwan and China could be soundless. Recent aggressions by Chinese warplanes to intrude in Taiwan's air defence identification zone (ADIZ) received broad attention; much less talked about, though equally threatening to Taiwan's security, is China's effort to encroach on Taiwan with cyberattacks. Over the past several years, many government agencies in Taiwan have fallen prey to such attacks. In 2020 alone, government agencies in Taiwan met 525 cybersecurity attacks.[1] The victims of those attacks have included high-value targets, like the presidential office[2] and major businesses in Taiwan, such as CPC (Chinese Petroleum Corp), damaging its customers' payment systems.[3] Mindful of the growing risks, the government of Taiwan has set up infrastructures and policies to meet future contingencies. This article begins by reviewing the development of Taiwan's cybersecurity structure at the government level before moving on to the risks and challenges the country faces. In the end, policy recommendations for the government to continue to strengthen its preparations are provided.

## THE DEVELOPMENT OF TAIWAN'S CYBERSECURITY

Taiwan's preparation for cybersecurity started quite early in 2000. The National Information and Communication Security Taskforce (NICST) under the Executive Yuan in Taiwan was the first governmental effort to combat cyber threats. The agency is tasked with protecting the government's networks and critical infrastructure. In addition to NICST, several other agencies gradually appear to enhance the government's cyber capability.[4]

Since the establishment of NICST, Taiwan has completed 4 phases of cybersecurity programs. The first two phases, from 2001 to 2004, and 2004 to 2008, laid the groundwork and completion for the country's cyber protection system. Another big task of these two phases is the classification of agencies to match each of them with different levels of cybersecurity threats and design corresponding strategies. From 2009–2012, the third phase built on existing preparations to seek cooperation with private sectors and raise awareness of the public. Local businesses were advised to adhere to cybersecurity laws and regulations and enhance their own cybersecurity systems. Education institutions at different levels started to roll out programs and offered classes related to cybersecurity. From 2013–2016, the fourth phase was devoted to fine-tuning government policies and regulations and spearheading the development of a cybersecurity industry and talent acquisition programs.[5]

From 2017–2020, the fifth phase was unparalleled in terms of depth and width of preparation. First, the issue of cybersecurity was elevated to the level of national security. In 2016, the National Information and Communication Security Office was established with the National Security Council (NSC). The NSC works closely and advises the president on national security affairs, indicating the government's level of awareness of cybersecurity concerns. In 2017, Taiwan set up the Information, Communication, and Electronic Force Command – the military arm to develop fundamental cybersecurity technologies and infrastructures. In 2018, to increase public awareness of cybersecurity, Taiwan's Congress (called the Legislative Yuan) passed the Information and Communication Management Act, offering guidelines and standard operating procedures for companies and government agencies to cooperate with relevant agencies on issues. In addition, this phase created a multilayered defence architecture including governmental sectors at various levels as well as local agencies. This phase also increased incentives to boost the cybersecurity industry, supporting at least 25 startups. Last, inter-agency collaboration also began to take place: the Ministry of Education (MOE) stepped up to take the burden of talent acquisitions. Until 2020, training programs set up by the MOE have resulted in 792 master and doctoral students and 96 pieces of industry-university cooperation.[6] For details about specific achievements of each phase, consult Figure 1.



- Define classification standard
- Promote implementation of cyber security management system
- The promotion of cyber security awareness

THE FIRST PHASE OF MECHANISM PLAN

Establish cyber security protection system; Complete rating system of governmental agencies

2001–2004

- Redefine classification standard; area of implementation extends to educational systems
- Implement national security operation center (SOC); provide regular surveillance and warning services
- Promote the system of chief information security officer

THE SECOND PHASE OF MECHANISM PLAN

Complete cyber security protection capabilities; Establish national security operation center

2005–2008

- Strengthen the implementation of various cyber security operation; plan a total of 30 action plans
- Enhance the completeness of cyber security regulations, for example: Personal Data Protection

THE THIRD PHASE OF DEVELOPMENT PROGRAM

Strengthen overall cyber security response capabilities; Refine report and response mechanism

2009–2012

- Complete united defense SOC platform
- Revised the "Government Agency (Institution) Cyber Security Responsibility Level Classification Operation Regulations

THE FOURTH PHASE OF DEVELOPMENT PROGRAM

Reinforce cyber security protection management united defense surveillance mechanism and cyber security information sharing

2013–2016

THE FIFTH PHASE OF DEVELOPMENT PROGRAM

Promote Cyber Security Management Act; Complete a national united defense system in cyber security

- Implement cyber security governance maturity model in government agency of cyber security responsibility
- Complete ISAC, CERT, SOC of critical infrasctructure
- Implementation of the "Cyber Security Industry Development Action Plan"

2017–2020

FIGURE 1: THE PROMOTIONAL PHASES OF CYBERSECURITY IN OUR COUNTRY[7]

## TAIWAN'S CYBERSECURITY CHALLENGES AND RISKS

The Internet provides both opportunities and challenges to all countries. Cyberattacks have been recognized as one of the potential risks, as indicated in World Economic Forum's (WEF) Global Risk Report.[8] Democratic governments, compared to autocratic ones, have less internet control, resulting in more cyber challenges.[9] Cybersecurity has already become a national security issue for nearly all democracies, including Taiwan. The openness of democracy's Internet environment provides foreign actors channels and opportunities to undermine democracy. Through cyber channels, foreign countries or actors can paralyze a target country's infrastructures, businesses, or transportation networks and spread disinformation or misinformation to undermine the target country's democracy and its civil society. Two of Taiwan's primary challenges that can undermine Taiwan's national security and democracy are cyberattacks and misinformation (plus disinformation).

According to Business Insider, misinformation refers to false or inaccurate information regardless of an intent to deceive.[10] For example, there was an online misinformation video saying that on October 12, 2021, many Taiwanese citizens walked on the streets asking for unification with China. According to the Taiwan FactCheck Center, this is exactly a piece of misinformation—no gathering happened on that day. This video came from a small-scale gathering in 2017 held by the Chinese Unification Promotion Party, a political party promoting Taiwan's unification with China. This video is also disinformation. What is disinformation, and what is the difference between disinformation and misinformation? Disinformation is a type of misinformation, according to Business Insider, that is intentionally false and intended to deceive or mislead.[11] The example above is also disinformation because it intentionally spreads false information that many Taiwanese people were eager to unify with China, trying to mislead the public.

In the following paragraphs, we focus on these two main threats and what lessons the Taiwanese government has learned.

## CYBERATTACKS

According to the National Institute of Standards and Technology, U.S. Department of Commerce, a cyber-attack refers to "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[12] So, this type of attack is virtual/digital in nature, but the consequence can be fatal, like traditional military attacks.

Why have cyberattacks become an increasingly severe concern for Taiwan? First, like in many other countries, in Taiwan, the Internet has become an essential component in running businesses, providing public service, and even defending the country. It is not hard to imagine that, if the network for businesses is interrupted or hacked, their intellectual properties could be leaked to impact profits negatively. If public service, such as electricity or transportation, is interrupted, chaos and panic among Taiwanese citizens would erupt. If Taiwan's defence capabilities are constrained by cyberattacks, then it would lower the cost for China to invade Taiwan. For example, if most of Taiwan's military radars and communication systems between military bases are shut down because of cyberattacks, then Taiwan will not be able to detect and respond to a Chinese invasion.

Second, there is evidence to suggest that China has been incessantly launching cyberattacks against Taiwan. According to Taiwan's digital minister, Audrey Tang, and Taiwan's minister of foreign affairs, Joseph Wu, Taiwan faces around 30 million cyberattacks per month—about 700 attacks per minute. Most of these cyberattacks originate from China.[13] Tang and Wu also mention that several of Taiwan's major petroleum and semiconductor companies, which are essential to Taiwan's economy, have been hacked by China; the U.S. and U.K. identified the origins of these attacks on Taiwan's important oil and semiconductor companies to likely be connected China's Ministry of State Security.

Because of Taiwan's unique political and economic situation of being threatened by China but producing the most advanced semiconductors worldwide, cooperating with like-minded countries to combat and deal with cyberattacks becomes way more important. According to the National

Cybersecurity Program of Taiwan (2021 to 2024), Taiwan's overall national cybersecurity united defence mechanism is not comprehensive yet, and the domestic cybersecurity industry is relatively small in scale, with insufficient output value, so it is important to cooperate with like-minded countries, such as the U.S. and Israel, to beef up Taiwan's cybersecurity industry.[14] Taiwan and the U.S. have started cooperating on cybersecurity issues. For example, in 2019, Taiwan and the U.S. held cybersecurity exercises, simulating threats posed by malicious actors. Besides, Taiwan and the U.S. also held the Global Cooperation and Training Framework (GCTF) Initiative, and a couple of the missions were put in place to strengthen cybersecurity and deter disinformation.[15]

## MISINFORMATION & DISINFORMATION

The second kind of cyber challenge or threat facing Taiwan is misinformation. Misinformation, in general, is not new for human beings. Before the appearance of the Internet, rumours or misinformation already existed. However, the Internet increases the speed and spread of misinformation, causing more serious concerns. In the U.S. and European countries, misinformation, especially disinformation, already impacts elections and democracy. For example, after analyzing 30 million tweets in the five months preceding the 2016 U.S. presidential election day, Bovet and Makse find that 25% of these tweets spread "either fake or extremely biased news." They also find that the activity of Trump's supporters influences the dynamics of top fake news spreaders.[16]

Likewise, in Taiwan, social media platforms, such as Line, WeChat, Facebook, and YouTube, accelerate the spread of all kinds of information, including misinformation. Misinformation or disinformation can spread faster when people are anxious or face uncertainty. Take the misinformation about COVID-19 vaccines in Taiwan as an example, which says that the AZ vaccines have serious side effects, and Moderna mRNA vaccines can impact human DNA and create fatal consequences. This fake news undermined Taiwanese citizens' faith in COVID-19 vaccines and lowered their vaccination willingness. President Tsai became aware of this issue and stated that fake news about vaccines were trying to reduce Taiwanese citizens' trust in Taiwan's Central Epidemic Command Center (CDC), the central agency handling all COVID-19 issues.[17]

According to Audrey Tang and Joseph Wu, Taiwan's digital and foreign affairs ministers, an estimated one-fourth of pandemic-related disinformation was believed to have come from China during the COVID-19 pandemic.[18] The openness of Taiwan's cyberspace provides malicious actors opportunities to sow confusion, chaos, and distrust in Taiwan society, eroding the stability of Taiwan's democracy. The Taiwan government has noticed this issue; most government websites now have an information clarification page, clarifying related fake news. Information clarification pages can provide a place for citizens to check the accurate information, but these pages are helpful only when people are willing to double-check the information they read; those who do not double-check the information may fall prey to fake news. So, as we elaborate in the recommendations sections below, increasing Taiwanese citizens' news literacy is an important mission for the Taiwan government to maintain the stability and health of Taiwan's democracy in the internet era.

## CYBERSECURITY POLICY RECOMMENDATIONS

Going forward, Taiwan can continue to strengthen its cybersecurity on multiple fronts. The latest version of the National Cybersecurity Program lays out several criteria.[19] We review these suggestions and offer our insights on how they could be strengthened. To begin with, one of the areas that the program focuses on is to attract high-level talents all over the world by increasing the number of cybersecurity instructors, devoting more resources to cybersecurity research, and recruiting talents from industry, academia, government, and military to enrol in training programs. These efforts have great potentials, and Taiwan does have an ample supply of talents working in the areas of information security and computer science abroad. We would like to see more synergies between agencies when rolling out specific action plans to incentivize these talents to contribute to the island's cyber defence. The program could include more details to explain how these efforts could be materialized.

The second area of effort revolves around the area of public-private partnerships. Most observes of Taiwan's cybersecurity industry would agree that their industry is rapidly growing, and the administration has been instrumental in creating a more friendly environment. In addition to the areas for cooperation, it is recommended to regularly conduct public-private united offensive and defence drills as laid out in the program. Experts from the industry can offer tangible suggestions, such as providing subsidies for business and education institutions to foster collaboration and talent acquisition, helping local companies become more competitive in the global market, and providing accreditation or other kinds of authentication systems to incentivize companies to comply with cybersecurity regulations.[20]

Taiwan's cyber ability can also be significantly boosted via improving collaboration with international partners. The United States has been a long-time partner on issues of cybersecurity. For instance, in 2019, the U.S. and Taiwan held the first joint cyber-war exercise known as the CODE (The Cyber Offensive and Defensive Exercises) drills. [21] In 2019, to foster talent exchange and acquisition, the Taiwanese authorities launched the Talent Circulation Alliance (TCA) with the American Institute in Taiwan (AIT).[22] In 2020, both sides held a cybersecurity Forum to exchange insights and strategies from the private sector.[23] In addition to continuing cooperation with the United States, the Tsai administration is also branching out to seek cooperation with other countries, such as Israel, that have tremendous expertise and experience in dealing with cyber-attacks[24]. Taiwan should certainly work with other states in other regions, such as the Baltic states, as they prepare for potential cyber threats from Russia.[25]

The last area of policy recommendation is to increase public awareness of cybersecurity. Efforts by the government and private sectors will be hampered if citizens are not aware of the potential threats. Survey evidence indicates that there is still room for improvement for public awareness in Taiwan. A 2017 survey by Consumers' Foundation asking over 2000 citizens found that only around 10% of citizens knew that they could see legal assistance when facing cybersecurity issues; 28% revealed that they could not verify if the payment method is safe when purchasing products online; only 40% of citizens considered cybersecurity when shopping online.[26] To help citizens prepare better, the Tsai administration could roll out regulations and pass new legislation to mandate citizens to be cognizant of threats in daily life. Relatedly, the administration could also increase funding and budgets to devote to public educational programs to bring the information to citizens proactively. For instance, the Ministry of Education has created a website[27] that introduces cybersecurity topics to citizens. More programs like this should be readily available. In a podcast interview, Taiwan's Digital Minister Tang also echoed the need for the government to find ways to make cybersecurity more accessible to citizens[28]. This is an area where positive results could trickle down to other areas mentioned above.

As discussed, cybersecurity is one of the critical challenges for Taiwan, as Chinese cyber warfare toward Taiwan is excessive and heinous. Though the Taiwanese government has prepared, we contend that some improvements are needed. It is equally important for Taiwanese citizens to be aware of these threats, recognize them, and be cautious to avoid being looped into their misinformation/disinformation framing.  We hope our chapter provides the foundation and can generate more awareness of this issue.

## ENDNOTES

[1] Lu, Y., Madjar, K., "Agencies hit by 525 cybersecurity threats last year", Taipei Times, 13.07.2021.

[2] Yang, S., "Taiwan Presidential Office hacked, documents linked to power struggle leaked", Taiwan News, 17.05.2020.

[3] Cheung, E., Ripley, W., Tsai, G., "How Taiwan is trying to defend against a cyber 'World War III'", CNN Business, 23.07.2021.

[4] "National Cyber Security Program of Taiwan (2021 to 2024)", National Information and Communication Security Taskforce, 08.06,2021, https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce.

[5] Ibid.

[6] Ibid.

[7] National Information and Communication Security Taskforce. Accessed on November 6, 2021, https://nicst.ey.gov.tw/Page/296DE03FA832459B/38cce861-6713-4b4c-bd2f-3c1900af4756.

[8] "Global Risks Report 2021", The World Economic Forum, 19.01.2021, https://www.weforum.org/reports/the-global-risks-report-2021.

[9] Sanger, D., Perlroth, N., "More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government", The New York Times, 19.07.2021.

[10] Gebel, M., "Misinformation vs. disinformation: what to know about each form of false information, and how to spot them online", Business Insider, 15.01.2021, https://www.businessinsider.com/misinformation-vs-disinformation.

[11] Ibid.

[12] Computer Security Resource Center. Accessed on November 6, 2021, https://csrc.nist.gov/glossary/term/cyber_attack.

[13] Tang, A., Wu, J., "Why Taiwan seeks Israel's help to combat cybersecurity threats", Jerusalem Post, 26.07.2021.

[14] "National Cyber Security Program of Taiwan (2021 to 2024) Report", National Information and Communication Security Taskforce, Executive Yuan, Taiwan, February 2021.

[15] "The Global Cooperation and Training Framework Programs", American Institute in Taiwan. Accessed on November 7, 2021, https://www.ait.org.tw/our-relationship/global-cooperation-and-training-framework-programs-gctf/.

[16] Bovet, A., Makse, H.A., "Influence of fake news in Twitter during the 2016 US presidential election", Nature Communication 10, 7, 2019, https://doi.org/10.1038/s41467-018-07761-2.

[17] Yeh, S., "Tsai Ing-wen: Fake news reduces people's trust in the CDC", Central News Agency, 07.07.2021, https://www.cna.com.tw/news/aipl/202107070198.aspx.

[18] Tang A., Wu, J., "Why Taiwan seeks Israel's help to combat cybersecurity threats", Jerusalem Post, 26.07.2021.

[19] "National Cyber Security Program of Taiwan (2021 to 2024)", National Information and Communication Security Taskforce, J 08.06.2021, https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce.

[20] Kuo, H. C., "Recommendations for Taiwan's Cybersecurity", 04.05.2021, https://buzzorange.com/techorange/2021/05/04/taiwan-data-security-industry-development/.

[21] "US and Taiwan Hold First Joint Cyber-War Exercise", BBC News, 04.11.2019, https://www.bbc.com/news/technology-50289974.

[22] "AIT Official Touts Talent Circulation Initiative", Taipei Times, 27.08.2019, https://www.taipeitimes.com/News/taiwan/archives/2019/08/27/2003721213.

[23] "Taiwan, U.S. Hold Cybersecurity Forum to Boost Collaboration, Exchanges", Ministry of Economic Affairs, 17.07.2020, https://www.moea.gov.tw/MNS/english/news/News.aspx?kind=6&menu_id=176&news_id=90615.

[24] Tang, A., Wu, J., "Why Taiwan seeks Israel's help to combat cybersecurity threats", Jerusalem Post, 26.07.2021.

[25] Patil, S., "The India-Taiwan Imperative for Cybersecurity Cooperation", Gateway House: Indian Council on Global Relations, 24.06.2021.

[26] "Citizens lacking Cybersecurity Awareness", Consumer' Foundation, Chinese Taipei, 26.04.2017, https://www.consumers.org.tw/product-detail-2696183.html.

[27] I Safe, https://isafe.moe.edu.tw/.

[28] "Interview with Audrey Tang", Infosec Decompress, 14.09.2020, https://infosecdecompress.com/pages/transcript_interview_with_audrey_tang.

# STRATEGIC COMMUNICATION

# THE ROLE OF STRATEGIC COMMUNICATIONS IN PREVENTING HYBRID THREATS IN THE BALTIC STATES

ELĪNA LANGE-IONATAMIŠVILI
Senior expert at the NATO Strategic Communications Centre of Excellence in Riga, Latvia

The three Baltic countries – Estonia, Latvia and Lithuania – recently celebrated one hundred years since the foundation of their independent republics. Their independence materialized in 1918, amidst the end of World War I that brought about new geopolitical realities in Europe. Half of these hundred years the three Baltic countries have spent under Soviet occupation, with the characteristic outcomes of totalitarian oppression, such as eradication of freedom of speech and press, mass deportations, arrests and murders of those perceived as dangerous to the occupying regime, a covert russification policy, and others.

In 1991, all three countries regained independence and were left with destroyed economies, changed ethnolinguistic composition, and soviet heritage in all spheres of life that required significant adaptation to align with Western ways of governance and development. Although it may have seemed at the time that the Russian Federation, the political heir of the Soviet Union, had changed course to become a democratic European state and a safe neighbour for the Baltic countries, it was not quite the case. As argued by Jukka Rislakki, Finnish journalist and author, Russia never truly intended to let the Baltic countries go. Soon after 1991, the Russian Federation embarked on multiple influence operations to distort history, deny occupation, damage the international image of the Baltic republics, gain control of business networks and core economic sectors, strengthen its influence in the national media, and the list goes on.[1] The Russian Federation has remained a top conventional threat for the Baltic countries since 1991, although the array of threats has broadened during the past three decades to include international terrorism, migration, cybersecurity, and information warfare, among others.[2]

In 2004, all three Baltic countries joined the North Atlantic Treaty Organisation (NATO) and the European Union (EU). This has led to a shared understanding of threats and a joint approach to tackling them, as reflected in the respective national security concepts of Estonia, Latvia, and Lithuania.[3] It also took away a significant advantage from Russia to influence domestic policies in these countries. Nevertheless, following the annexation of Crimea by the Russian Federation in 2014, strong security concerns in this part of the world remain, which have resulted in NATO stationing its international troops, the Enhanced Forward Presence, in the Baltic states and Poland.

The geopolitical context and historical experience have kept the Baltic countries on a constant alert. Throughout three decades, Russia has used coercive methods through control of energy supplies and demonstration of cyber and military power, sharp power through influence in business and domestic politics, and soft power through information campaigns, primarily targeting local Russian language speakers[4]. Baltic states do not believe a conventional military conflict to be an immediate reality in relations with Russia, although such possibility always remains on the radar.[5] The countries are, however, highly concerned with the potential of hybrid threats designed not to cross a clear response threshold,[6] and particularly with hostile influence in the cognitive domain of their societies.

## THE CHANGING UNDERSTANDING OF SECURITY: PRIORITIZING THE COGNITIVE DOMAIN

Following the events in Crimea, all Baltic countries have revised their approach to national security. All three recognize the threat to the cognitive domain as a major challenge for a country's security and highlight the need for the whole of society to be resilient. For example, Estonia uses the term ‘broad security concept’ in its National Security Concept (2017). It is defined as “the ability of a state and its people to defend its intrinsic values and objectives from the various external political, military, economic and social threats and risks and their combined impact, as well as the capability to neutralise those threats and risks”.[7] This speaks to the understanding that the core target of an adversary is the cognitive domain of Estonian society. In the National Security Concept of Latvia, internal security policy is described as “reliant on a strong civil society that has a unified understanding about its value orientation, the identity of the Republic of Latvia regarding the Western world.”[8] Latvia’s concept reflects closely on cyberspace and information space as priority areas to prevent threats to national security. Lithuania’s National Security Strategy also highlights the ‘information threats’ which can lead to distrust in state institutions, undermine democracy and Lithuania’s NATO and EU membership, and seek to widen societal divides in order to weaken national identity.[9]

Although all three documents use different wording, the core idea is the same: unless we can protect the cognitive domain of our societies from hostile foreign influence, we risk a distorted understanding of democratic values. That, in turn, can lead to undemocratic choices in elections and a fragmented society unable or unwilling to recognize and resist foreign hostile influence. It leaves the country vulnerable to hybrid attacks in particular, due to their ambiguous nature.[10]

The concept of cognitive warfare holds a prominent place in the current security discourse. As suggested by NATO’s Innovation Hub’s Cognitive Warfare Project, ‘Information Warfare and Cognitive Warfare will probably become permanent courses of action to obtain the desired end state which is the destabilization of a political leader, an enemy force, a country, or even an Alliance.’[11] In cognitive domain operations, information is used to influence target country’s cognitive functions, ranging from peacetime public opinion to wartime decision-making.[12] It is designed to manipulate the public discourse in a target country, seeking to undermine social unity or damage public trust in the political system, and destabilize the country.[13]

## THE RELATIONSHIP BETWEEN HYBRID THREATS AND STRATEGIC COMMUNICATIONS

The establishment of the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland in 2017, warmly welcomed by the EU and NATO, demonstrated the increased importance that Western democracies attach to understanding the changing nature of the security environment. The Centre has become a focal point for research and policy advisory on hybrid threats, and all three Baltic countries contribute their expertise to it. To an extent, Finland and the Baltic countries share the historical experience regarding Russia. Although Finland's strategic approach to its relationship with Russia differs from that of the Baltic countries, Finland remains concerned with developments inside Russia and its military and foreign policy.[14] The Centre defines hybrid threats as actions conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state, or institutional level.[15] That resonates with the definition of cognitive warfare, explained above. Importantly, the definition of hybrid threats goes on to say that such actions are coordinated and synchronized, and deliberately target state and institutional vulnerabilities.[16] This brings us to the concept of strategic communications and its role in pre-empting hybrid threats.

Strategic communications, as defined by NATO's Strategic Communications Centre of Excellence, is understood as "a holistic approach to communication based on values and interests that encompasses everything an actor does to achieve objectives in a contested environment".[17] This definition implies that the cognitive domain is constantly being contested by a variety of actors. It also conveys that strategic communications sits at the core of policy-making and implementation. It is a mindset that allows to conduct statecraft through the projection of values-based narratives and implementing policies through aligned words and actions to ensure the consolidation of democracy, appropriate levels of national security, and cohesion and welfare of the whole of society. The problem of hybrid attacks lies within their ambiguity and multi-faceted character, complicating attribution and response.[18] Often it is not possible to determine the origin of a hybrid attack or to instantly grasp the scale of the attack across different domains. A strong strategic communications approach means decreased vulnerabilities of the country as a whole, and can be seen as a pre-emptive action to hybrid attacks. The establishment and operation of the European Centre of Excellence for Countering Hybrid Threats in itself can be seen as an act of strategic communications. It is a symbolic demonstration of a shared understanding of the problem and joint work to tackle it. At the same time, it also sends a signal to adversaries that participating countries are decreasing vulnerabilities and developing new ways of detection and response which may serve as a deterrent to future attacks.

The problem with defining and implementing strategic communications lies in the broadness of the concept. It foresees not only horizontal coordination in a whole-of-government approach but also a vertical thread ensuring coherence through all levels of policymaking and implementation, starting from the highest political level down to the tactical level. Nevertheless, such an approach where the country's efforts to develop and strengthen itself politically and militarily are seen as a joint coordinated effort, instead of thinking and operating in silos, is crucial for deterrence of hybrid threats which are often designed to target different domains simultaneously.

## STRATEGIC COMMUNICATIONS AND HYBRID THREATS IN THE BALTICS

The Baltic countries have been developing their understanding of strategic communications alongside the rest of the democratic West for the past two decades. Being part of NATO and the EU, the Baltic states have been influenced by the developing understanding of the strategic communications concept in these two organisations. One of the key developments has been the recognition that strategic communications is not an operational or tactical level activity employed to communicate policies *post factum*. The strategic communications function sits next to the political leadership of the country and spreads out across government departments and in the military through designated personnel and structural units.

Currently, all three countries as Parliamentary democracies employ strategic communications cells within the Government offices, directly subordinated to the Prime Ministers. That ensures continuous close engagement with the highest level of policy-makers and active participation in policy-making. The role of strategic communications in the Government offices, with the help from other institutions and outsourced services, is to monitor and analyse the information environment (national and international), provide respective insight to the policy-makers, and, based on this insight, advise on strategic communications approach and concrete steps. The steps taken can range from communications campaigns (for example, on the centenary of independence) to infrastructure projects (for example, Rail Baltica). The information environment can be understood as dynamic physical and/or virtual settings interpreted by the mind.[9] The effects of strategic communications seek to achieve a cognitive effect in target audiences, by either action or inaction, communication or silence. In order to choose the best course of action for a cognitive effect, it is of utmost importance to have an understanding not only of the media environment but also of the audiences and discourses that exist in the society outside of the media.

As discussed above, Russia remains the main concern for the Baltic countries in terms of security. RAND Corporation's report on Russia's hybrid threats in the Baltic countries identifies potential non-violent political subversion as the main challenge.[20] The report emphasizes that the ability of the local population to resist Russian cognitive warfare, accompanied by other instruments of influence, is crucial for a successful response to hybrid attacks. Therefore, a greater priority should be placed on increasing the resilience of the targeted societies to political subversion.

The globalized information space and rapid development of information technologies have diminished the confidence and capacity of states to secure and control events, and the Baltic countries are no exception.[21] In this context, resilience-building requires the awareness of insecurity or contingency, which allows to look for ways how a society can bounce back from disturbances that cannot necessarily be predicted.[22] It implies moving away from the traditional state-centred approaches to problem-solving, and looking for building relationships and networks that could alert and help tackle changes in the security environment.[23] This thinking is also reflected in the policies implemented by the Baltic countries, which are increasingly moving towards a whole-of-society approach to defence and security. But there is still a long way to go.

The Russian-speaking populations, largely concentrated in Estonia and Latvia,[24] have been identified as vulnerable to Russia's hostile influence attempts in the information space.[25] The key vehicles of influence have been the Kremlin-controlled TV channels, a leading source of information for the Russian-speakers, and locally-based pro-Kremlin non-governmental organisations and political parties[26].

All three Baltic countries have taken decisive steps to limit Russia's influence in the cognitive domain. For one, Latvia and Lithuania have banned the Kremlin-controlled TV channels for the spread of hate speech and disinformation.[27] All countries have worked hard to strengthen independent media, including in the Russian language. Estonia's ETV+ channel is one such example, with a growing local audience.[28] The Baltic Centre for Media Excellence is another case where countries have pulled resources together to educate journalists, strengthen regional media, analyse audiences, and promote media literacy to citizens.[29] The last round of Parliamentary elections[30] saw thorough preparations for hostile influence and disinformation attempts, resulting in increased cooperation between government agencies and mass media, as well as Facebook and Twitter. Nevertheless, the problem of Russia's influence in the cognitive domain remains an issue, making the Baltic countries voice their concerns also within the EU format.[31] The establishment of the East StratCom Task Force in 2015 is one tangible result that works towards raising awareness and thus limiting Russia's disinformation activities in the region.

But one should not assume that the vulnerability of the Baltic countries lies only with the Russian-speaking populations. The ongoing COVID-19 pandemic has demonstrated how quickly societies can become polarized over an issue. Although Russia has employed overt and covert disinformation campaigns to undermine Western-manufactured vaccines[32], the anti-vaccination and anti-government movement spread across the whole of society.[33] Russia's disinformation activities may have had a certain impact, but by large the Baltic countries are faced with faults in their strategic communications, leading to more coercive strategies than elsewhere in the Nordic-Baltic region. The effectiveness of the vaccination process, as well as levels of compliance with government regulations, correlate with the levels of trust in the government and the socio-economic conditions within a country.[34] That is why we have to return to the understanding of strategic communications as statecraft oriented on the long-term shaping of discourses through the implementation of corresponding policies.

## THE EXAMPLE OF ESTONIA: STRATEGIC COMMUNICATIONS VICTORY OVER A HYBRID ATTACK

The most significant hybrid attack experienced in the Baltic countries has been the 2007 cyberattack on Estonia. This internationally well-known case demonstrates how Estonia employed strategic communications against the backdrop of a crisis. Crisis communication does not stand outside of strategic communications; it is not seen as separated from the overarching values and goals of a country, the existing discourses, or the country's understanding of security. Although the decision-making process is condensed and adapted for crisis response, the country bears the fruit of its strategic communications to date. A country can rely only on existing resources (including the discursive ones) which open persuasion and coercion avenues to handle a crisis. And the way how a crisis is handled will affect its future strategic communications perspectives.

Let us explore the example of Estonia in more detail. After regaining independence in 1991, Estonia had to look for ways to rebuild its economy. The visionary political decision to digitalise Estonia enjoys widespread domestic support to this day and has become a central part of Estonia's official country image and branding.[35] Before joining the EU in 2004, Estonia had embarked on its Tiger Leap and X-road projects for the digitalisation of education, governance and services. That became the backbone of the e-Estonia nation brand.[36] The sharp turn to digital Estonia was possible due to strong political leadership through different governments, distributed data architecture and strategy, central strategic guidance and financial controls, and decentralised implementation through public-private networks to pull the best expertise together.[37] This serves as an excellent example of a country's strategic communications.

In 2007, Estonia's highly digitalised but ethnically and linguistically split society[38] became an attractive target for a hybrid attack from Russia. In response to Estonia's decision to relocate the Soviet Bronze Soldier monument away from the centre of Tallinn, Russia mounted a three-week-long cyberattack on government institutions and private businesses. Although the Russian government denied involvement, the vast majority of malicious network traffic was of Russian origin and had indications of political motivation.[39] The cyberattack was accompanied by protests organised by a local Russian pro-Kremlin organisation *Nochnoy Dozor*[40] that turned into two nights of riots and looting. Their actions were supported by *Nashi* in Moscow, a pro-Kremlin group that has official Russian government endorsement.[41] *Nashi* sieged the Estonian embassy, adding a new pressure point.[42]

In this hybrid attack, Russia targeted two potential vulnerabilities: the high dependency on digital technologies and the collective memory of the local Russian population in Estonia (and in Russia), who do not share the Estonian interpretation of history. Estonia showed agility in responding to the cyberattack by quickly pulling together public and private resources. This was in line with how Estonia had been developing before the crisis: strong informal networks linking private, non-governmental and public sectors were at the core of the country's rapid digital advancement.[43] Importantly, it decided to focus its communication efforts on drumming up the international community's support, rather than on reacting to the rhetoric coming from Russian politicians and media.[44] For Estonia, it was clear that the support from Western allies would be decisive in this long-term battle.

Estonia saw the crisis as a strategic opportunity. It established the Cooperative Cyber Defence Centre of Excellence, which has become an important hub for expertise within NATO. It used events in Estonia as reasoning to advance NATO's policymaking in the area of cyber defence and hybrid threats. As Josh God puts it, Estonian officials "spun the unprecedented attacks into a calculated narrative, seeking to frame them not as a classic Russia-versus-Estonia story, but as a newly emerging global security challenge to all."[45] This is a great example of strategic communications, whereby Estonia emerged from the crisis as a world-renowned expert in cybersecurity. Estonia managed to influence the international discourse on Russia, and the policy-making in the greatest political-military alliance in history. All of that would not have been possible without the hard work Estonia had been putting in domestically for two decades before the crisis struck – not only in building a digital country with strong national networks but also by fostering its strategic international relationships.

But there is always a drop of tar in the pot of honey. As discussed earlier, a large part of the Russian-speaking minority in Estonia continues to live in the Russian, mainly Kremlin-controlled, media space.[46] The Russian state network *Rossiya* remains the most watched.[47] In the opinion of Estonian strategic communications expert Raul Rebane, "the fact that Russian networks shape the minds of so many people in Estonia is nothing short of dangerous".[48] Until this vulnerability is addressed through more effective integration and media policies, it can be targeted again in the future.

## WAY FORWARD FOR THE BALTICS

For small countries that do not rank among the world's top economies, conducting effective strategic communications nationally and internationally is easier said than done. Back in 2004, the Baltic countries already made the most important strategic steps to date by joining NATO and the EU. However, both these organisations recognize that their cohesion should not be taken for granted: any alliance is as strong as its weakest link. NATO's 2030 report emphasizes that the shared democratic norms and identities of NATO members underpin the endurance of the Alliance.[49] Same goes for the EU; the souring of the relationship with Poland over the EU's founding treaty principles is a recent example.[50] For the Baltic countries, faced with a neighbour like Russia, the best security guarantee against hybrid threats is to be exemplary members of these two international organisations.

First and foremost, it means being exemplary democracies. An important component of that is strong and independent national media, which is particularly hard to achieve, given the small market that remains linguistically divided. Secondly, it means developing cohesive, well-educated and prosperous societies that are satisfied with the government's services in the broader understanding. Recent research on Latvia demonstrates how the consolidation of liberal European values, increased stability, and economic development can result in the desired change in public opinion among young Russian speakers.[51]

As to hybrid threats, Russia with its current political leadership will remain the main source of threat in the Baltics in terms of cognitive warfare, accompanied by cyberattacks or other irregular warfare elements. To this end, the Baltic countries have already made several important steps to strengthen national information and cyberspace. But several challenges remain. One step is the integration of the Russian-speaking minorities and their rotation towards national media space instead of that controlled by the Kremlin. That is directly linked to the level of state language knowledge as well as the provision of high-quality media content in the minority languages. Closing down foreign TV channels is not a long-term solution, unless a viable local alternative is offered.[52]

The other step is the strategic development of the three countries, ensuring strong, future-oriented nation-branding for domestic audiences. Estonia stands out in this regard, having developed from the outset the identity of a modern digital country, and supporting it with well-resourced long-term policies. Digital Estonia is not only a fancy façade to be employed in international relations. It makes everyday life better for all citizens. One of the main narratives promoted by Russia to Baltic audiences is that of a 'failed state'.[53] For this narrative to gain traction, Russia is not only being inventive with disinformation but also appeals to the lack of national vision and jumps at opportunities provided by real-life problems in each country. The continuous exposure to such a narrative can bring about the loss of will to protect the country and its democratic values. And that is how a victory in cognitive warfare looks like for Russia.

Last but not least, the three Baltic countries could capitalize on the Nordic-Baltic cooperation format which was established after 1991. The

COVID-19 crisis demonstrated that although there was little strategic cooperation between the Baltic countries as well as the Baltic and Nordic countries, the region benefited from commonly developed financial stability instruments, found joint ways for repatriation of citizens, and worked together to develop digital solutions to the crisis.[54] The creation of the Baltic Bubble, the first of the kind common area of free movement in pandemic-struck Europe, became a symbol of the political unity of the Baltic countries in a crisis and reminder of close inter-connectivity.[55] As discussed, a crisis serves as an illustration of the success or failure of long-term strategic communications. The region is facing similar threats: Russian and Chinese influence and cognitive warfare. Although China is not a front-runner in the public information space and uses different tactics to Russia[56], the eight countries in the region could benefit from closer cooperation on addressing these threats. The Baltic countries could also strengthen their democracies by strategically increasing integration with their Nordic neighbours who are achievers in the world ratings on freedom of media, among other areas. Latvia, for one, is emphasizing the Nordic identity in government communications. But words have to be consistently backed up by deeds to bring positive change in our societies and decrease vulnerabilities.

## ENDNOTES

[1] Rislakki, J., "The Case for Latvia: Disinformation Campaigns Against a Small Nation", Amsterdam, New York: Editions Rodopi B.V., 2008.

[2] "National Security Concept of Estonia", Ministry of Defence of the Republic of Estonia, 2017, https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.; "National Security Concept of Latvia", Ministry of Defence of the Republic of Latvia, 2019, https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.; "National Security Strategy of Lithuania", Ministry of National Defence of the Republic of Lithuania, 2017, https://kam.lt/download/57457/2017-nacsaugstrategijaen.pdf.

[3] Ibid.

[4] Russian language speakers are understood as ethnic Russians and other ethnic minorities residing in the Baltic countries for whom the primary language of communication is Russian.

[5] "National Security Concept of Estonia", Ministry of Defence of the Republic of Estonia, 2017; "National Security Concept of Latvia", Ministry of Defence of the Republic of Latvia, 2019; "National Security Strategy of Lithuania", Ministry of National Defence of the Republic of Lithuania, 2017.

[6] "Strategic Communications Hybrid Threats Toolkit", Gill. M., Heap, B., Hansen, P., (eds.), NATO Strategic Communications Centre of Excellence, 08.09.2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

[7] "National Security Concept of Estonia", Ministry of Defence of the Republic of Estonia, 2017.

[8] "National Security Concept of Latvia", Ministry of Defence of the Republic of Latvia, 2019.

[9] "National Security Strategy of Lithuania", Ministry of National Defence of the Republic of Lithuania, 2017.

[10] "Strategic Communications Hybrid Threats Toolkit", Gill. M., Heap, B., Hansen, P., (eds.), NATO Strategic Communications Centre of Excellence, 08.09.2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

[11] "Cognition Workshop: Innovative Solutions to Improve Cognition", NATO's Innovation Hub's Cognitive Warfare Project, June 2021, https://www.innovationhub-act.org/sites/default/files/2021-07/210601%20Cognition%20Workshop%20Report-%20v3.pdf.

[12] Beauchamp-Mustafaga, N., "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," China Brief, Vol. 19, No. 16, Jamestown Foundation, 2019, https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/.

[13] Bjørgul, L.K., "Cognitive warfare and the use of force", Strategem, 03.11.2021, https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/.

[14] Lavikainen, J., "Russia's redefined view on strategic stability: A security dilemma in Northern Europe?", Finnish Institute of International Affairs, 16.04.2021, https://www.fiia.fi/en/publication/russias-redefined-view-on-strategic-stability; Moshes, A., Nizhnikau, R., "Three decades of Russian policy in the European part of the post-Soviet space: Swimming against the current", Finnish Institute of International Affairs, 11.11.2021, https://www.fiia.fi/en/publication/three-decades-of-russian-policy-in-the-european-part-of-the-post-soviet-space.

[15] "Hybrid Threats as a Concept", The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[16] Ibid.

[17] Bolt, N., Haiden, L., "Improving NATO Strategic Communications Terminology", NATO Strategic Communications Centre of Excellence, June 2019, https://stratcomcoe.org/publications/improving-nato-strategic-communications-terminology/80.

[18] "Hybrid Threats as a Concept", The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[19] Bolt, N., Haiden, L., "Improving NATO Strategic Communications Terminology", NATO Strategic Communications Centre of Excellence, June 2019, https://stratcomcoe.org/publications/improving-nato-strategic-communications-terminology/80.

[20] Radin, A., "Hybrid Warfare in the Baltics: Threats and Potential Responses", RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR1577.html,

[21] "The Routledge Handbook of International Resilience", Chandler, D., Coaffee, J., (eds.), 2017, London; New York: Routledge, p. 1–6.

[22] Ibid.

[23] Ibid.

[24] Out of the three Baltic countries, in Latvia and Estonia there are about 25% ethnic Russians, in Lithuania about 5%.

[25] Bērziņa, I., Cepurītis, M., Juurvee, I., Kaljula, D., "Russia's Footprint in the Nordic-Baltic Information Environment 2016/2017", NATO Strategic Communications Centre of Excellence, January 2018, https://stratcomcoe.org/publications/russias-footprint-in-the-nordic-baltic-information-environment-20162017/138; Radin, A., "Hybrid Warfare in the Baltics: Threats and Potential Responses", RAND Corporation, 2017.

[26] "Annual Review 2020/2021", Estonian Internal Security Service, 2021, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202020-2021.pdf.: *"2020.gada pārskats",* State Security service, 2020, https://vdd.gov.lv/lv/?rt=documents&ac=download&id=58.

[27] "More Russian TV channels have the plug pulled in Latvia", LSM.lv, 09.02,2021 https://eng.lsm.lv/article/features/media-literacy/more-russian-tv-channels-have-the-plug-pulled-in-latvia.a392163/.; "Lithuanian media watchdog moves to ban Russian TV channel for incitement to war", LRT, 29.10.2020, https://www.lrt.lt/en/news-in-english/19/1264184/lithuanian-media-watchdog-moves-to-ban-russian-tv-channel-for-incitement-to-war.

[28] Bahovski, E., "First Steps towards the Estonian Media Space", International Centre for Defence and Security Studies, 02.04.2020, https://icds.ee/en/first-steps-towards-the-estonian-media-space/.

[29] "Our Work", Baltic Centre for Media Excellence, https://bcme.eu/en/our-work/.

[30] Parliamentary elections took place in Latvia in 2018, in Estonia in 2019, in Lithuania in 2020.

[31] Kalniete, S., "Draft Report of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation", European Parliament, 18.10.2021, https://www.europarl.europa.eu/doceo/document/INGE-PR-695147_EN.pdf.

[32] Gordon, M.R., Volz, D., "Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say", The Wall Street

Journal, 07.04.2021, https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200.

[33] "Who spreads the vaccine lies in the Baltics?",  RE:Baltica, 28.02.2021, https://en.rebaltica.lv/2021/02/who-spreads-the-vaccine-lies-in-the-baltics/.

[34] Bolt, N., Engebretsen, I., Lange-Ionatamišvili, E., Michelsen Forsgren, M.K., Sayed, R., "How Did The Nordic-Baltic Countries Handle The First Wave of COVID-19?" NATO Strategic Communications Centre of Excellence, July 2021, https://stratcomcoe.org/publications/how-did-the-nordic-baltic-countries-handle-the-first-wave-of-covid-19/211.

[35] Kattel, R., Mergel, I., "Estonia's digital transformation: Mission mystique and the hiding hand", Institute for Innovation and Public Purpose, September 2018, https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/iipp-wp-2018-09_estonias_digital_transformation.pdf.

[36] "Interoperability services", E-Estonia. https://e-estonia.com/solutions/interoperability-services/x-road/.

[37] Ibid.

[38] Loit, U, Harro-Loit, H., "Media Pluralism Monitor 2016: Monitoring Risks for Media Pluralism in the EU and Beyond. Country Report: Estonia", Centre for Media Pluralism and Media Freedom, December 2016, https://cmpf.eui.eu/media-pluralism-monitor/mpm-2016-results/estonia/.

[39] Heap, B., Krauel, S., Althuis, J., et. al. "2007 cyber attacks on Estonia", NATO Strategic Communications Center of Excellence, https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

[40] Vedler, S., "Money from Russia: Divide and Conquer Estonia" Re:Baltica, 18.03.2012, https://en.rebaltica.lv/2012/03/divide-and-conquer-in-estonia/.

[41] Mijnssen, I., "The Quest for an Ideal Youth in Putin's Russia I: Back to Our Future! History, Modernity and Patriotism according to Nashi, 2005-2013", Stuttgart: Ibidem-Verlag, 2014, p.104.

[42] Lowe, C., "Russian protesters "lay siege" to Estonian embassy", Reuters, Moscow, 03.05.2007, https://www.reuters.com/article/uk-estonia-russia-scene-idUKL0354549820070503.

[43] Kattel, R., Mergel, I., "Estonia's digital transformation: Mission mystique and the hiding hand", Institute for Innovation and Public Purpose, September 2018, https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/iipp-wp-2018-09_estonias_digital_transformation.pdf.

[44] Author's conversation with the Spokesperson of the Estonian Ministry of Foreign Affairs, Tallinn, December 2007.

[45] Gold, J., "How Estonia uses Cybersecurity to Strengthen its Position in NATO", International Centre for Defence and Security, 27.05.2019, https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/.

[46] Dougherty, J., Kaljurand, R., "Estonia's "Virtual Russian World": The Influence of Russian Media on Estonia's Russian Speakers", International Centre for Defence and Security, 13.11.2015, https://icds.ee/en/estonias-virtual-russian-world-the-influence-of-russian-media-on-estonias-russian-speakers/.

[47] Ranne, R., "Russian propaganda pouring into the brains of Estonian viewers", Postimees, 02.11.2021, https://news.postimees.ee/7376088/russian-propaganda-pouring-into-the-brains-of-estonian-viewers.

[48] Ibid.

[49] Williams, M, C., Neumann, I.B., "From Alliance to Security Community: NATO, Russia, and the Power of Identity", Millennium: Journal of International Studies, SAGE Journals, Vol. 29, No.2, https://doi.org/10.1177/03058298000290020801, p. 357–387.

[50] Auer, S., Scicluna, N., "Poland has a point about the EU's legal supremacy", Politico, 19.10.2021, https://www.politico.eu/article/poland-court-eu-legal-supremacy/.

[51] Kugel, M., Lisenkov, A., *"Different from both their parents and Latvian peers. Latvian Russian-speaking youth choose liberal freedoms, EU values and are satisfied with NATO membership – research by Spektr. Press and SKDS"*, Spektr.press, 10.10.2011, https://spektr.press/different-from-both-their-parents-and-latvian-peers-latvian-russian-speaking-youth-choose-liberal-freedoms-eu-values-and-are-satisfied-with-nato-membership-research-by-spektr-press-and-skds/.

[52] *"Mediju eksperte: Vairāku Krievijas TV kanālu aizliegšana Latvijā var aizkaitināt daļu sabiedrības; jāpiedāvā alternatīvas",* LSM.lv, 10.02.2021, https://www.lsm.lv/raksts/zinas/latvija/mediju-eksperte-vairaku-krievijas-tv-kanalu-aizliegsana-latvija-var-aizkaitinat-dalu-sabiedribas-japiedava-alternativas.a392275/.

[53] "Russia's Footprint in the Nordic-Baltic Information Environment 2019/2020", Lange-Ionatamishvili, Elina (ed.), NATO Strategic Communications Centre of Excellence, November 2020, https://stratcomcoe.org/publications/russias-footprint-in-the-nordic-baltic-information-environment-20192020/24; Ruduša, R., *"Sārts: Viltus ziņās Latviju aizvien cenšas attēlot kā neizdevušos valsti",* LSM.lv, 04.03.2017, https://www.lsm.lv/raksts/zinas/latvija/sarts-viltus-zinas-latviju-aizvien-censas-attelot-ka-neizdevusos-valsti.a226581/.

[54] Bolt, N., et al. "How Did The Nordic–Baltic Countries Handle The First Wave of COVID-19?" NATO Strategic Communications Centre of Excellence, July 2021.

[55] "Coronavirus: Baltic states open a pandemic 'travel bubble'", BBC, 15.05.2020, https://www.bbc.com/news/world-europe-52673373.

[56] Bērziņa-Čerenkova, U., Bohman, V., Lucas, E., Svetoka, S., "China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden", NATO Strategic Communications Centre of Excellence, November 2021, https://stratcomcoe.org/pdfjs/?file=/publications/download/Executive-summary-Chinas-influence-in-the-Nordic-Baltic-FINAL-32653.pdf?zoom=page-fit.

# STRATEGIC COMMUNICATION: THE CASE OF TAIWAN

**J. MICHAEL COLE**
Taipei-based Senior Fellow at the Global Taiwan Institute in Washington, D.C., the Macdonald-Laurier Institute in Ottawa, Canada, and the Taiwan Studies Programme at the University of Nottingham, UK

Although the Chinese military represents a serious and undeniable threat to Taiwan's national security, the Chinese Communist Party (CCP) nevertheless continues to aim for conditions in which the use of force, and the many unknowns attendant to the decision to initiate major military operations against Taiwan, are not necessary. Following Sun Tzu, the Chinese leadership would much prefer to win without having to fight. In order to do so, it must create a sense of embattlement, of inevitability and of defeatism, among the targeted society and government. It is a state of perpetual conflict, where the frontiers between war and peace are continually blurred. These aims, and the instruments utilized to achieve those non-kinetic objectives, are the object of this paper.

Before we go any further, it is important that we clearly define what is meant by "hybrid warfare" and what this strategy entails in the context of the Taiwan Strait. Orenstein defines "hybrid war" (sometimes referred to as "political warfare," "grey area warfare," or "new-generation warfare") as:

> a coordinated system of military and non-military (political, diplomatic, legal, economic, ideological, scientific-technical and others) measures taken consecutively or simultaneously [...] entailing damage of a strategic character [...] designed in a way to evade detection and to create a facade of plausible deniability [...] an all-out assault on [...] institutions, conducted largely by covert methods in order to escape notice and avoid provoking a strong response.[1]

For his part, Hoffman argues that "hybrid warfare" manifests itself when "any adversary [...] simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the same time and battlespace to obtain their political objectives."[2]

In the Chinese context, the term "hybrid warfare" often has been conflated with the "Three Warfares" – public opinion warfare, psychological warfare, and legal warfare – a concept that became famous after the Chinese leadership revised the "Political Work Guidelines of the People's Liberation Army" in 2003. However, as Mattis notes,[3] the "Three Warfares" are related to the People's Liberation Army (PLA) and therefore should be regarded as a subset to, rather than the organizing principle of, the Chinese Communist Party's (CCP) hybrid/political warfare strategy.[4] By strictly looking at PLA activity, we risk missing out on various elements of CCP influence operations that are not primarily handled by the PLA. The "hybrid warfare" strategy discussed in this paper, therefore, is to be regarded as the sum of activities implemented as part of the overarching strategy set by the Chinese People's Political Consultative Congress (CPPCC).[5]

It should therefore be noted here that the term "battlespace," to which Hoffman refers in his definition, is not limited to the military arena but instead the full spectrum of activities of which the military is but one element. Where PLA activity is mentioned in this paper, it is primarily in instances where its uses are intended as an instrument of political warfare. Consequently, the more traditional aims of military activity, such as training, are not discussed.

## AIMS OF CHINA'S "HYBRID WARFARE" STRATEGY AGAINST TAIWAN

China's "hybrid warfare" against Taiwan constitutes a sustained, coordinated and multidimensional effort to erode its target's ability to withstand annexation. Among its key objectives, the CCP seeks to undermine state cohesion, democratic institutions, public support for democracy as their system of governance, exacerbate polarization, sow confusion, and create a sense of inevitability with regards to the ultimate "reunification" of Taiwan with “the mainland.” Although some elements of China’s “hybrid warfare” strategy utilize overt instruments, such as the uses of PLA exercises and transits near Taiwan to wage psychological warfare against the Taiwanese public and create a sense of embattlement, much of this “hybrid warfare” is waged by means which provide a modicum of plausible deniability.

China’s “hybrid warfare” efforts are directed against: (1) Taiwanese society, its government and institutions; and (2) the external environment in order to shape conditions within the international system in ways that are favourable to Beijing’s designs upon Taiwan.

On the domestic front, the area where Chinese “hybrid warfare” has arguably met the greatest success is that of polarization. This is facilitated by pre-existing conditions within Taiwanese society stemming from Taiwan’s history – the “mainlander” versus “Taiwanese” ethnic divide on the one hand, and the Democratic Progressive Party (DPP) versus Chinese Nationalist Party (KMT) on the other. This longstanding schism has prevented the formation of a united front to resist external aggression, while creating numerous opportunities for the CCP to engage in co-optation and elite capture. Beijing has encouraged those divisions and has sought to exacerbate them, often by using history and culture to reinforce the “shared destinies” of the two peoples (Taiwanese as “compatriots,” those who refuse unification regarded as “traitors”).

Taiwan’s heavy reliance on the Chinese market and the close interdependence that has developed between the two countries’ economies over the past decades, have also been conducive to such activities. Beijing has exploited this phenomenon by making one’s ability to conduct business, or, in the case of artists, to perform in the PRC, contingent on the person’s (or firm’s) willingness to become complicit in China’s political efforts against Taiwan.[6]

Although it is difficult to quantify success when it comes to “hybrid warfare,” there are nevertheless some areas where Beijing has succeeded in shaping the environment in favour of its political objectives. Chief among them is the notion that “reunification” is a historical inevitability against which only a small number of Taiwanese, primarily within the DPP, along with “outside forces,” are militating. The result of propaganda, co-optation, Chinese funding and endowments, disinformation, and coercion, such conditioning has successfully framed the "Taiwan issue" as one of "separatism" rather than what is: a matter of annexation. Related to this effort are Beijing's successes in creating confusion in foreign capitals, academia, think tanks, the media and the private sector, about a country's "one China" *policy* – in which a government normally "takes note of" Beijing's claims of sovereignty over Taiwan – and Beijing's "one China" *principle,* which states that Taiwan is part of the PRC. Over decades, this element of China's "hybrid warfare" has succeeded in isolating Taiwan, excluding it from multilateral institutions, and led academic institutions, publishers, and private firms to engage in risk-avoidance by avoiding Taiwan as a topic. Chinese officials elected to head U.N. specialized agencies (or co-opted officials from other countries) have also used their position to frustrate efforts by Taipei and international partners to secure Taiwan's meaningful participation.[7] Additionally, over the years there have been many instances of on-campus intimidation of Taiwanese students by PRC students, Chinese Students and Scholars Association (CSSA) chapters, as well as Chinese embassies and consulates.[8] This has often resulted in reluctance on the part of Taiwanese students to participate in cultural events or to promote their country of origin.

The CCP has also been relatively successful in fostering the narrative on the international stage that support for Taiwan is "anti-China," the result of a "cold war mentality," the remit of "right-wing" organizations, or the machinations of Western intelligence agencies and the military-industrial complex. Another related narrative has it that Taiwan is a mere pawn of the U.S. among efforts to contain or encircle China, and that Taiwan is as much a threat to China military as China is to Taiwan ("false threat-symmetry"). Consequently, the Left and Libertarians in the West have been vehemently opposed to any form of assistance to Taiwan, from diplomatic recognition to the provision of defence articles or military assistance. Many intellectuals within the "abandon Taiwan" camp are found within such organizations, which in several instances have also been co-opted, consciously or not, by the CCP.[9]

Other areas of "hybrid warfare" activity (see Section III below) have met variable success, their impact mitigated by the resilience of Taiwan's institutions, a mobilized civil society that is ready to take action whenever the government is perceived to be acting unaccountably, and arguably the CCP's inability to fully comprehend the nature of Taiwanese society.

## MEANS OF CHINA'S 'HYBRID WARFARE' STRATEGY AGAINST TAIWAN

China deploys a vast array of instruments to wage "hybrid warfare" against Taiwan. Although it is beyond the scope of this paper to provide an exhaustive list of all the entities and instruments that are involved in such activities against Taiwan, the following are among the most prominent:

> **PLA coercion:** Incursions into Taiwan's air defence identification zone (ADIZ)[10] or across the tacit "median line" in the Taiwan Strait[11]; live-fire exercises combined with official propaganda (PLA, Taiwan Affairs Office, state media) to exacerbate the sense of embattlement (psychological warfare) or to depict such manoeuvres as responses to "provocations" by Taiwan and/or its allies. China's ostensibly civilian "maritime militia" has also been deployed in waters near Taiwan's outlying islands to whittle away at Taiwan's territory, and to swarm and confuse Taiwan's Coast Guard Administration.
>
> **Dis/misinformation:** Cognitive warfare by Chinese state media outlets, UFWD-linked outlets (e.g., Voice of the Strait, *China Review News*), PLA-linked outlets (e.g., Base 311 (also known as Unit 61716), trolls, "sock puppets," PRC-funded content farms/mills in Taiwan, Facebook, Youtube channels, Line groups, pro-Beijing traditional media in Taiwan, politicians, and influencers;[12] co-optations of traditional and new media via cross-Strait media forums in Beijing and Xiamen[13]; uses of dis/misinformation to sow confusion, undermine belief in objective reality, and exploit tensions caused by elections, referenda, electoral recalls, and controversial issues (e.g., COVID-19 vaccines, food products from the U.S. or Fukushima Prefecture) to exacerbate polarization.
>
> **Economic carrots and sticks, trade weaponization:** Lure of the Chinese market, preferential treatment for Taiwanese nationals (e.g., Fujian's Pingtan experimental free-trade zone) in return for favours; tourism, purchasing delegation to municipalities governed by the KMT

or politicians who recognize the "1992 consensus" versus denial for those governed by the DPP; punitive trade measures (e.g., a boycott of imports of pineapple and other fruit from Taiwan in 2021[14]); bypassing of central government institutions for cross-Strait trade and direct outreach by pro-CCP entities to Taiwanese farmers, fishermen associations, etc.[15]

**Co-optation:** Recruitment of party-affiliated (often fringe) or independent politicians, businessmen, media conglomerates, influencers, entertainers; all-expenses-paid trips to China for academics, students ("Communist Party schools") and journalists where recruitment or indoctrination are attempted; positions at Chinese universities or research centres; uses of cultural organizations (often serving as fronts for UFWD entities) for cross-Strait forums where "shared culture" and "shared destiny" are inevitable themes; religious groups (Taoist temples), cross-Strait visits, Matsu pilgrimage.

**Pro-CCP "civil society":** Organizations such as the Patriot Alliance Association, ROC (CPAROC), retired military personnel groups including 800 Heroes, Blue Sky Alliance, and Kao An-kuo's Republic of China Taiwan Military Government have been used to promote unification, intimidate Taiwanese society, government officials and occasionally Hong Kong activists. Whether acting independently or at the orders of the CCP, such entities threaten social stability (the Republic of China Taiwan Military Government can in fact be regarded as a militia, although at this writing the threat appears to be more aspirational than real[16]).

**Pro-Beijing political parties:** Legally registered, these include the China Unification Promotion Party (CUPP, the Taiwan Red Party (TRP) and New Party, whose members openly advocate for unification and "one country, two systems." Those organizations have been scrutinized by the authorities over suspicions surrounding their sources of funding (e.g., illegal funding from the PRC). Party members are known to have associated with and participated in conferences organized by UFWD-linked entities overseas (e.g., the China Council for the Promotion of Peaceful Reunification, CPPRC).[17]

**Organized crime:** A symbiotic relationship has developed between the CCP, pro-CCP organizations and organized crime ("triads") in Taiwan, primarily with the Bamboo Union and the Four Seas Gang. Led by former Bamboo Union head Chang An-le (aka "White Wolf"), the CUPP has often mobilized members of the Bamboo Union, along with *jiaotou* ("corner heads") to intimidate Taiwanese civil society, provide protection for

> visiting senior Chinese officials, or physically assault critics of the CCP. One recent assassination attempt against an outspoken Taiwan advocate has involved members of the Bamboo Union, with financing coming from the PRC.[18] The Bamboo Union is also heavily involved in arms trafficking, thus giving its members access to various firearms that could be used should the organization be ordered to create social instability, engage in sabotage, and so on. Funding for those groups comes from their criminal activity (gambling dens, prostitution, arms smuggling, debt collection) as well as underground banking from the PRC. The overlapping of criminal activities and political work creates a particularly challenging blind spot for law enforcement and intelligence agencies, which tend to compartmentalize their efforts and sharing of information.[19]

## TAIWAN'S STRATCOM RESPONSES AND RECOMMENDATIONS

This section discusses Taipei's strategic communication (stratcom) responses to the PRC's hybrid threat. According to Cornish, Lindley-French and Yorke, strategic communication in the context of national security

> comprise[s] four main components: information operations; psychological operations; public diplomacy; and public affairs. These in turn contain common elements. First is the need to inform, influence and persuade audiences at home and abroad, whether friendly, adversarial or merely a member of the public. Second is the need to promote coordination across government to avoid what the US Army calls 'information fratricide'. Third, the need to communicate strategically is itself dependent on the ability to communicate actions to all affected and interested audiences and to ensure that actions are themselves communicable, i.e. complementary to and supportive of strategic objectives.[20]

Taiwan's stratcom response to the PRC's "hybrid warfare" has been a longstanding weakness. Only recently, under the Tsai Ing-wen administration, has this challenge received the government attention that it needed, and there are still doubts as to whether Taipei's strategy is sufficiently coordinated. One recent example of a clear stratcom success on Taiwan's part is the decision by the Ministry of National Defense (MND) to use its Twitter account to provide data and charts about daily PLA incursions into Taiwan's southern ADIZ, an effort that generated tremendous attention worldwide when the PRC substantially increased such activity in October 2021.[21]

Other initiatives, such as the recent launching of the government-sponsored TaiwanPlus, an English-language TV platform, are also part of ongoing efforts to position Taiwan internationally, for a fraction of the cost of similar outlets by Beijing, such as CGTN.[22]

Ironically, Taiwan's stratcom efforts have received assistance from an unexpected corner: China. Beijing's growing assertiveness and belligerence under Xi Jinping, perhaps best illustrated by the undiplomatic behaviour of its "Wolf Warrior" diplomats abroad, has benefited Taiwan by encouraging countries around the world to reassess their China policy and, by rebound, the value of Taiwan to their own national interest. The COVID-19 pandemic has also given Taiwan an unexpected opportunity to demonstrate the value and resilience of its political system and industries, and to provide much-needed medical assistance in the early phase of the pandemic.

Amid a growing clash of ideologies, Taiwan's role as a front-line state in this battle between the liberal-democratic order and authoritarian revisionism is being recognized in ways that would have been unimaginable just a decade ago. This, in turn, has created a unique moment for Taiwan to use stratcom to counter China's "hybrid warfare" and to shape the global environment in its favour.

As it develops and strengthens its countervailing stratcom efforts, Taipei must seek to:

- Debunk the notion that the Taiwan Strait is a "domestic" matter for all Chinese, an "unfinished civil war," that unification is a "historical inevitability" and that Beijing is being compelled to respond "defensively" to "provocations" by Taiwan and the international community. Clarify that PRC claims are annexationism and that its ambitions would be destabilizing to the region as a whole and the liberal-democratic world order;
- Overturn the CCP narrative that only a small number of pro-independence members of the DPP and external allies oppose "re-unification";

- Debunk the notion, formulated and broadcast by the CCP, the Western ideological left and CCP proxies that only the "right-wing," defence contractors and intelligence agencies support Taiwan. This necessitates much greater engagement by Taiwan with think tanks and media that uncritically internalize and spread such perceptions;
- Counter the false narrative of "threat-symmetry" in the Taiwan Strait expounded by the CCP and various supporters in China and abroad, which argues that Taiwan also represents a military threat to China through the acquisition and deployment of offensive weapons. Greater effort must be made to explain that Taiwan is acting in a purely defensive fashion and that it long ago abandoned its ambitions to "retake the mainland";
- Demonstrate that the PRC can hone its hybrid warfare instruments against Taiwan and subsequently turn them against other members of the democratic alliance. This includes maritime militias, substate actors, organized crime, cyber, dis/misinformation, co-optation, elite capture, et cetera;
- Implement an all-of-society endeavour to collaborate with international partners on combating political warfare, dis/misinformation, cyberattacks, pro-CCP sub-state actors, and so on;
- Counter sustained efforts by the PRC to portray Taiwanese as unwilling to defend themselves and that they are passively waiting for the American cavalry to save them. Besides a public diplomacy campaign, this also necessitates defence reform (including the formation of a proper Reserve Force) and greater emphasis on asymmetry. This constitutes an example of stratcom through action, in this case through a demonstrable commitment to national defence, and would go a long way toward countering efforts by Taiwan's enemies to discredit the military;
- Demonstrate willingness on the part of law enforcement and intelligence agencies to sanitize classified information pertaining to hybrid warfare activities so as to make those public. To facilitate such an effort, an intelligence fusion centre, modelled on the UK's Joint Intelligence Committee (JIC), should be created to collect and analyse all-source intelligence for the preparation of threat assessments, in both

classified and declassified formats. This would help the government make its case for strengthened national security laws and enforcement, while serving as material for its international outreach. This would also help counter claims by opposition politicians and CCP proxies that Taipei is inflating the threat. A divided society that cannot agree on the seriousness of an external threat is inherently weakened and will appear less credible when interacting with international partners);

- Create a stratcom coordination committee at the National Security Council (NSC), with principals from all the key agencies involved in national security (MND, National Security Bureau, Ministry of Justice Investigation Bureau, Executive Yuan, National Police Agency, Ministry of Foreign Affairs), to maximize the effectiveness of Taiwan's responses to Chinese "hybrid warfare" and appropriate dissemination to a domestic and international audience;
- Increase participation at various international fora where hybrid warfare is the object of discussion. This includes, but is not limited to, the G7 Rapid Response Mechanism, Halifax International Security Forum, Shangri-La Dialogue, Munich Security Conference, Raisina Dialogue, Forum 2000, and so on, as well as Track 1, 1.5 and 2 exchanges with foreign governments and academic institutions. Use the strategic opportunity created by current conditions in the international system to host conferences and attract foreign civil society, media, and investment. Such platforms should also be used to emphasize the role of Taiwan as a member of the community of democracies, with a greater focus upon non-traditional allies such as the Baltic states as well as Central and Eastern Europe;
- Substantially increase government funding for Taiwan's film industry, production and distribution, to increase the presence of Taiwanese movies, documentaries, and other mediums on the international stage as part of its "soft power" strategy. Promote Taiwan's fiction and non-fiction by making translated works about Taiwan more accessible in Taiwan (bookstores, popular tourist spots, ports of entry) and abroad.

# CONCLUSION

This paper provides an overview of the various instruments used by the CCP to undermine, erode, and thereby weaken Taiwan's ability to sustain its sovereignty and defend itself against Chinese annexationist claims. As Beijing constantly adapts its strategy to achieve its objectives, a shifting global environment punctuated by rising scepticism of China's intentions has created opportunities for Taiwan to counter the longstanding Chinese narrative on the Taiwan Strait. Although Taipei has made progress in using stratcom to improve its visibility and reputation within the international community at a time when China's has suffered, years of institutional neglect on Taiwan's part and limited receptivity to its plight within the international community mean that Taiwan is now playing catch-up. Its stratcom strategy, therefore, remains too ad hoc and underfunded. The areas highlighted in Section IV constitute a starting point for areas that are ripe for exploitation and which could further strengthen Taiwan's ability to counter Chinese hybrid warfare. Besides mitigating the detrimental effects of Chinese hybrid warfare, Taiwan's stratcom strategy must move beyond a purely reactive approach and instead become more proactive, with the aim of shaping the environment and global discourse in its favour.

## ENDNOTES

[1] Orenstein, M.A., "The Lands in Between: Russia Vs. the West and the New Politics of Hybrid War", New York: Oxford University Press, 2019, p. 179n41.

[2] Hoffman, F., "On Not-So-New Warfare: Political Warfare vs Hybrid Threats", War on the Rocks, 28.07.2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

[3] Mattis, P., "China's 'Three Warfares' in Perspective", War on the Rocks, 30.01.2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

[4] The same applies to the PLA's Strategic Support Force (SSF) created in 2015 amid reorganization "to create synergies between disparate information warfare capabilities in order to execute specific types of strategic missions that Chinese leaders believe will be decisive in future major wars." See Costello, J., McReynolds, J., "China's Strategic Support Force: A Force for a New Era", National Defense

University Center for the Study of Chinese Military Affairs Institute for National Strategic Studies, China Strategic Perspectives, No. 13, October 2018, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[5] Mattis, P., "The Center of Chinese Influence: The Chinese People's Political Consultative Conference", in "Insidious Power: How China Undermines Global Democracy", Szu-chien, H., Cole, J.M., (eds.), Manchester Eastbridge, 2020, p. 3–39.

[6] Horton, C., "How Beijing enlists global companies to pressure Taiwan", Nikkei Asia, 25.07.2018, https://asia.nikkei.com/Spotlight/The-Big-Story/How-Beijing-enlists-global-companies-to-pressure-Taiwan.

[7] Trofimov, Y., Hinshaw, D., O'Keeffe, K., "How China Is Taking Over International Organizations, One Vote at a Time", Wall Street Journal, 29.09.2020, https://www.wsj.com/articles/how-china-is-taking-over-international-organizations-one-vote-at-a-time-11601397208.

[8] Off-the-record interviews with the author.

[9] For a good example of this, see Goldstein, L.J., "How progressives and restrainers can unite on Taiwan and reduce the potential for conflict with China", Quincy Institute for Responsible Statecraft, 17.04.2020, https://responsiblestatecraft.org/2020/04/17/how-progressives-and-restrainers-can-unite-on-taiwan-and-reduce-the-potential-for-conflict-with-china/.

[10] "56 China military planes enter Taiwan's ADIZ, setting another record", Focus Taiwan, 04.10.2021, https://focustaiwan.tw/cross-strait/202110040027.

[11] "Taiwan under psychological attack as Chinese warplanes cross median line, analysts say", South China Morning Post, 03.10.2020, https://www.scmp.com/news/china/diplomacy/article/3103985/taiwan-under-psychological-attack-chinese-warplanes-cross.

[12] "China Using 'Cognitive Warfare' Against Taiwan, Observers Say", Voice of America, 17.01.2021, https://www.voanews.com/a/east-asia-pacific_china-using-cognitive-warfare-against-taiwan-observers-say/6200837.html.

[13] Cole, J. M., "More Than 70 Participants From Taiwanese Media Industry Attend 4th Cross-Strait Media Summit in Beijing", Taiwan Sentinel, 11.05.2019, https://sentinel.tw/more-than-70-participants-from-taiwanese-media-industry-attend-4th-cross-strait-media-summit-in-beijing/.

[14] "Taiwan threatens to take China to WTO in new spat over fruit", Reuters, 19.09.2021, https://www.reuters.com/world/china/china-halts-taiwan-sugar-apple-wax-apple-imports-prevent-disease-2021-09-19/.

[15] "United Front Target Taiwan's Grass Roots: Gangs, Temples, Business", Common Wealth Magazine, 22.08.2018, https://english.cw.com.tw/article/article.action?id=2083.

[16] 【退將成立台灣軍政府　正式向台灣民政府宣戰】, Apple Daily, 28.02.2018,

https://tw.appledaily.com/politics/20180228/ACSYPORJWPDG4GDQT-DZG5QBTPA/. See also Cole, J. M., "CCP Proxies Call for Mutiny, Violence, and Overthrow of the Tsai Government", Global Taiwan Brief, Vol. 6, No. 16, 11.08.2021, https://globaltaiwan.org/2021/08/vol-6-issue-16/#JMichaelCole08112021.

[17] Cole, J. M., "*Cross-Strait Relations Since 2016: The End of the Illusion*", London: Routledge, 2020, p. 52-4.

[18] 【獨/反共惹禍?知情曝館長遭中國買凶】,Set TV, 08.10.2020, https:// tw.news.yahoo.com/ 獨 - 反共惹禍 - 知情曝館長遭中國買凶 -120029563.html.

[19] Cole, J. M., "On the Role of Organized Crime and Related Substate Actors in Chinese Political Warfare Against Taiwan", Ministry of Justice Investigation Bureau, Prospect and Exploration, June 2021, https://www.mjib.gov.tw/FileUploads/eBooks/6f2646ebb06a4ddba2449c950a42533d/Section_file/8a0b255919bc48e1bc3d2a38825cd3c8.pdf.

[20] Cornish, P., Lindley-French, J., Yorke, C., "Strategic Communications and National Strategy", Chatham House report, https://www.chathamhouse.org/sites/default/files/r0911es–stratcomms.pdf.

[21] The official twitter account of the Ministry of National Defense of the Republic of China, https://twitter.com/MoNDefense.

[22] TaiwanPlus, https://www.taiwanplus.com.

# ABOUT THE AUTHORS

**UNA ALEKSANDRA BĒRZIŅA-ČERENKOVA** is Head of the Asia program at the Latvian Institute of International Affairs, and a member of the European Think tank Network on China. Dr. Bērziņa-Čerenkova has studied at Beijing Language University, Beijing Normal University et.al. After having defended her doctoral dissertation on traditional Chinese discourse in Hu Jintao's report to the 17th National Congress of the Communist Party of China, she has held a Senior visiting research scholar position at Fudan University School of Philosophy, Shanghai, China (2014/15) and a Fulbright visiting scholar position at the Center for East Asia Studies, Stanford University, USA (2019/20).

**SINTIJA BROKA** is a Researcher and Project manager at the Latvian Institute of International Affairs and a Ph.D. candidate in political science at Rīga Stradiņš University. Sintija Broka holds a bachelor's degree in International Economics from the University of Latvia and a master's degree in International Relations and Diplomacy from Rīga Stradiņš University. She has recently worked as a visiting Ph.D. fellow at the University of Ghent and economic researcher at the United Arab Emirates Embassy in Riga. She is currently studying Arabic studies at the Middle East Institute in Washington. Sintija Broka's academic interests include the Middle East political and economic sustainability, religion and politics in the Middle East, as well as the policy dynamics of the Gulf region.

**J. MICHAEL COLE** is a Taipei-based senior fellow with the Global Taiwan Institute in Washington, D.C., the Macdonald-Laurier Institute in Ottawa, Canada, and the Taiwan Studies Programme at the University of Nottingham, UK. He holds a Master's Degree in War Studies from the Royal Military College of Canada and is a former intelligence officer with the Canadian Security Intelligence Service. His latest book, Insidious Power: How China Undermines Global Democracy (co-edited with Dr. Hsu Szuchien) was published in 2020.

**IVO JUURVEE** is Head of Security & Resilience Programme and Research Fellow at the International Centre For Defence and Security. Ivo Juurvee had been a practitioner in the field of security for more than 13 years. Amongst other positions in Estonian public service, he has been an adviser at the National Security and Defense Coordination Unit of the Estonian Government Office and the head of the Internal Security Institute of the Estonian Academy of Security Sciences. He has also taught security-related topics at the University of Tartu, Estonian Military Academy, Estonian School of Diplomacy, Diplomatic Academy of Ukraine, NATO School (Oberammergau), and FRONTEX master's program on border management. Ivo's professional and academic areas of interest are information warfare, intelligence services, and other forms of hybrid conflict. He has worked as an Honorary Research Fellow at University College London, School of Slavonic and East European Studies, and given a guest lecture in several universities, including Stanford and Georgetown. He holds a Ph.D. degree in history from the University of Tartu (2013) and an MA from the Central European University, Budapest (2003). Ivo is an author of two books and numerous articles and reports.

**ELINA LANGE-IONATAMIŠVILI** is a senior expert at the NATO Strategic Communications Centre of Excellence in Riga, Latvia. She has been a defence civil servant for eight years, four of which she spent in Georgia running a NATO trust fund for professional development and reform support. Her previous jobs include heading the Public Diplomacy Division at the Ministry of Defence of Latvia and working on public diplomacy projects under the NATO Riga Summit 2006 Task Force. She holds MA in Communication Science (2006) and MA in Audio-Visual and Stage Arts (2020). Currently Elina is a Ph.D. student at the King's College London, War Studies Department, researching the role of memory construction in strategic communications.

**CHIA-YI LEE** is an Associate Professor at the Department of Diplomacy, National Chengchi University in Taiwan. Prior to NCCU, Chia-yi Lee was an assistant professor at the S. Rajaratnam School of International Studies, Nanyang Technological University in Singapore. Chia-yi Lee obtained her Ph.D. from the Department of Political Science at Washington University in St. Louis. Her research interests include international political economy, energy and resource politics, foreign direct investment, terrorism, and political methodology. Chia-yi Lee has published in prestigious international journals such as International Studies Quarterly, Journal of Conflict Resolution, Journal of Peace Research, and Review of International Organizations.

**HSUAN-YU (SHANE) LIN** is currently a pre-doctoral research fellow in the Fairbank Center for Chinese Studies at Harvard University and a Ph.D. Candidate in the Department of Politics at the University of Virginia. His research focuses on public opinion, social media, international security, and U.S.–Taiwan–China relations and is funded by the Democratic Statecraft Lab at the University of Virginia, the Fulbright Program, and the Harvard Fairbank Center. Mr. Lin received his B.A. and M.A. from the Department of Political Science at National Taiwan University.

**VIDA MACIKENAITE** is an Assistant Professor at the International University of Japan. She holds graduate degrees from Keio University in Japan and Fudan University in China. While her major field of research is Chinese domestic and foreign policies, she is also interested in authoritarian regimes and state capacity in comparative perspective.

**ANDRIS SPRUDS** is the Director of the Latvian Institute of International Affairs. He also holds the position of professor at Riga Stradins University. Andris Spruds has an MA in Central European History from the CEU in Budapest, Hungary and in International Relations from University of Latvia. He has also obtained a Ph.D. in Political Science from Jagiellonian University in Krakow, Poland. Andris Spruds has been a visiting student and scholar at Oxford, Uppsala, Columbia and Johns Hopkins University, as well as the

Norwegian Institute of International Affairs and Japan's Institute of Energy Economics. His research interests focus on energy security and policy in the Baltic Sea region, the domestic and foreign policy of post-Soviet countries, and transatlantic relations.

**LOUIS JOHN WIERENGA** is a Junior Research Fellow in Comparative Politics at the Johan Skytte Institute of Political Studies, University of Tartu and Lecturer in International Relations at the Baltic Defence College. Previously he has held guest fellowships at Uppsala University's IRES (Institute for Russian and Eurasian Studies), Sodertorn University's Department of Political Science; and with the Chair of Comparative Politics at European University Viadrina Frankfurt (Oder). Louis has also held guest lecturer positions at the University of Latvia and the Tallinn University of Technology (TalTech). Louis's research interest include populist radical right parties - specifically leadership and party structure, social media and discursive opportunity structures, youth organizations, transnational networks, foreign policy, and social movement parties and metapolitical actors and their engagements between ideology and party structures.

**CHARLES K.S. WU** is an Assistant Professor in the Department of Political Science and Criminal Justice at South. His primary research interests fall into the intersection between International Relations and American Politics, and his research agenda focuses on the factors that influence public opinion on military operations overseas. Dr. Wu's academic and policy work has been published in Social Politics, Scientific Data, Journal of East Asian Studies, Journal of Asian and African Studies, International Relations of the Asia-Pacific, The National Interest, The Diplomat, and The Pacific Forum. His latest coauthored book is Presidentialism, Violence, and the Prospect of Democracy (Lexington Book, 2021).

**YAO-YUAN YEH** is Chair of the Department of International Studies & Modern Languages, Director of the Master of Diplomacy & Strategic Affairs Program, Assistant Coordinator of the Taiwan & East Asia Studies Program, and Associate Professor of International Studies at the University of St. Thomas, Houston. His research focuses on public opinion, foreign policy, international security, US-China-Taiwan relations, East Asian politics, terrorism and political violence, and quantitative methods. Dr. Yeh's academic and policy work has been published in various prestigious platforms, including but not limited to British Journal of Political Science, Terrorism and Political Violence, The China Quarterly, Social Science Quarterly, Scientific Data, International Relations of the Asia-Pacific, The Defense Post, THE DIPLOMAT, East Asia Forum, and The National Interest. He has coedited a volume titled Taiwan: The Development of an Asian Tiger (Lynne Rienner Publishers, 2019) and coauthored in Presidentialism, Violence, and the Prospect of Democracy (Lexington Book, 2021).

LATVIAN INSTITUTE OF
INTERNATIONAL AFFAIRS

The Latvian Institute of International Affairs (LIIA) is the oldest Latvian think tank that specializes in foreign and security policy analysis. LIIA was established in 1992 as a non-profit association with the aim of providing Latvia's decision-makers, experts and the wider public with analysis, recommendations and information about international developments, regional security issues, and foreign policy strategies and choices. It is an independent research institute that conducts research, develops publications and organizes public lectures and conferences related to global affairs and Latvia's international role and policies.

21 Pils Street, Riga, LV-1050 | www.liia.lv