Global Conversations

War and Peace:

A Tapestry of Conflict and Resolution

Winter Edition 2024

Table of Contents

Our Team

Dear Readers,

It is with great pleasure that we introduce to you our latest issue, "War and Conflict: A Tapestry of Conflict and Resolution." This year has unfolded with an array of intense and defining moments that have reshaped international landscapes and tested our collective resilience, whether that be the war in Gaza, or the conflict in Ukraine. From escalating military engagements to complex geopolitical manoeuvres, the narratives of war and conflict continue to weave through the fabric of our global interactions.

In this issue, we delve into the multifaceted and often contentious intersections of war, diplomacy, and resolution. Our writers have explored topics ranging from the ethical quandaries faced by private military contractors to the impactful role of drones in the ongoing Russia-Ukraine conflict. We examine how settler colonialism plays out across different global contexts, and analyze the intricate propaganda of China, and the role this played on Taiwan's recent elections. Additionally, we provide insights into the volatile situation in Myanmar with rebels challenging the military coup, and unpack the growing menace of ransomware attacks in our increasingly digital world.

As the shadows of conflict continue to loom large, understanding these complex dynamics is crucial for forging paths toward peace and resolution. We hope the essays and analyses in this issue enrich your understanding of these critical issues and stimulate thoughtful dialogue.

We trust that you will find this collection of essays as enlightening and thought-provoking as we have.

Editors-in-Chief,
Adhithya Krishnan and Dan McDowall

Merging Business and Battlefield:

Moral Dilemmas of Privatized Military.

By Steffi Hebel. Edited by Aurora Schatz.

Merging Business and Battlefield:

Moral Dilemmas of Privatized Military.

At the onset of the Iraq War in 2003, for every ten US military service members, there was one private military contractor (PMC). As the US pulled out of Afghanistan in 2020, there were more contractors than actual US military service members, a factor of 1.5:1 to be exact. Many other states have resorted to the use of PMCs as political instruments, for foreign policy objectives, or what is regarded as immoral military campaigns. One thing is clear: PMCs are the new frontiers of war and have become a business.

PMCs, or mercenaries, are the private sector of war. A PMC is prepared to carry out a full-on military offensive under a contract. Putting conflicts at wholesale paves a future that is a dystopian nightmare. From a moral standpoint, there are certain things that armies do - and a way of doing them - that simply should not be in the private sector. PMCs are not fighting for their state, for duty, nor for patriotism. The bottom line is that the motivation for fighting is happening solely for profit.

As Max Weber cleverly wrote in his Politics as a Vocation, "the state is a human community which (successfully) claims the monopoly of the legitimate use of force". What is put into question is one word - legitimate. What now constitutes the legitimate use of force, and who gets to decide? In 2020, PMCs had an estimated global market value of $223 Billion USD. This is merely the known economic activity; there is no "valuation day" in the PMC industry. Hence, this figure is likely to be much larger and is projected to double by the year

Oftentimes, highly skilled former military professionals are attracted to PMC positions as they are competitively bid and financed projects. Yet, it would be a myth to assume that most contractors are aligned with the governments they are working for. In reality, they often have opposing goals. This is because PMCs operate in the shadows; lacking any sense of transparency and accountability.

In the age of information, plausible deniability becomes a lucrative reality for those who are willing to pay the right price. On one hand, this has arguably helped prevent conflict escalation. Political and military leaders can place blame on "mercenary groups", claim plausible deniability, and thus keep interstate conflict at bay. On the other hand, the lack of accountability and international regulatory law means PMCs could very literally get away with murder.

Central to concerns about international law are the following issues for consideration: legitimacy and accountability, state sovereignty, performance, threats to peace and stability, and post-conflict realities. The latter, post-conflict realities, are an under-examined feature by decision makers. Although PMCs have low long-term operational costs compared to state militaries, PMCs often profit privately from war locally. The bottom line? The negative externality cost is shifted to the public in the communities they are operating in. The non-economic costs and consequences are also large and mostly overlooked. The price of negative social externalities is seldom factored into the cost

Merging Business and Battlefield:

Moral Dilemmas of Privatized Military.

of using PMCs.

There are generally three different models of PMCs: the South African Model, the US Blackwater Model, and the Wagner Model. The South African Model is based on the highly controversial company, Executive Outcomes (EO). EO operated as traditional mercenaries, often financing their expenditures from resource extraction in the countries they were in. The US Blackwater Model is different in its approach, often regarded as military entrepreneurship with frequent state partnerships. The Blackwater Model has become increasingly influential since the post-Cold War era of subcontracting and privatizing US forces. Blackwater also played a large role in what the US regards as their war against terrorism. Lastly, the Wagner Model is a frightening divergence from these prior two models. The Wagner Group operates largely with impunity and has had a formal link established with the Kremlin. It is organized in a network that has partnered with organizations that have influenced US and European elections by propagating false information. As it appeared, the Wagner Group was loyal to the Kremlin. Until it was not. An attempted coup resulted, and the world's most foreseeable plane crash.

Scholars question the topic of allegiance. Considering how PMCs are frequently used as political instruments, several questions are raised. Does the "corporation for hire" have a foreign policy of its own? Is that PMC's foreign policy in sync or in opposition to their government's foreign policy objectives? Who exactly are they working for when there is allegiance to seemingly no state? Given the Wagner Group's attempted Kremlin Coup, it would appear there are more questions than answers.

Considering the current trend of PMC expansion, it is worth asking whether the next military superpower will be a country, or a corporation. In a perfect world, it would be up to the public to decide if the use of force by a nonstate actor is appropriate. In the world we live in, this is not the case. State decision makers must start putting some lines down in the sand and safeguard against PMC risks, human rights abuses, and government manipulation. The danger is not just the PMCs, but also state ineptitude in strategy and preparedness.

By Steffi Hebel. Edited by Aurora Schatz.

The Drone War:

A look into the impact of UAVs in the Russia-Ukraine War.

By Andrew McKay. Edited by Cameron Vrckovnik.

The Drone War:

A Look Into the Impact of UAVs in the Russia-Ukraine War

Initial Drone Technology

The Russia-Ukraine War is now into its third calendar year, and dynamic, adaptive technologies are becoming more prevalent than ever on the battlefield. As Ukrainian and Russian forces continue to battle for an edge in the conflict, one of the most necessary fronts for victory is that of drone supremacy.

In the initial stages of the war, Ukraine relied heavily on more traditional military drones, notably, the Turkish Bayraktar TB2. This particular drone provided Ukraine the opportunity to evade Russian air defenses and hit fortified targets. However, Russian countermeasures developed defense systems to detect and neutralize these larger military drones. In the wake of these Russian advancements, Ukraine was forced to shift its focus toward smaller drones that could go undetected by Russian systems.

Throughout the war, Ukraine has purchased and received drones from foreign countries; however, the conflict created a necessity for domestic drone manufacturing. Since Russia's invasion in February of 2022, the number of private Ukrainian drone manufacturers rose from seven to eighty. Mykhailo Fedorov, Deputy Prime Minister of Ukraine, said that the Ukrainian government has spent more than USD 1 billion on drones in the year 2023, and that "we have increased production more than 100 times since last year (2022)." Presently, common Ukrainian drones include the A1-CM Fury, ASU-1 Valkyrja, and Leleka-100.

Innovation and Adaptation

A large part of Ukrainian strategy has also involved tapping into the commercial drone market where drones can be purchased for less than USD 1,000. Commercial drones typically used for racing and videography have been repurposed for surveillance and single-use strikes. Most of these commercial drones are First Person View (FPV) drones . They have two main functions: reconnaissance and striking. Those that strike targets are loaded with a grenade or shell and can be commanded by a drone pilot nearby. The rationale for using these drones is simple: cheap drones, expensive targets. At around 150 km/hour, these drones still manage to hit their targets with precision. Only five months into the war, the Ukrainian government began crowdsourcing commercial drones to test and experiment their combat-readiness. Many Ukrainian civilian engineers have been recruited by the government to aid in the war effort by modifying commercial drones into battle-ready unmanned aerial vehicles (UAVs). This has introduced a breadth of ideas, specifications, and new innovations in drone technology at a faster pace than through traditional military procurement.

Russia's drone strategy on the other hand, has been heavily affected by Western sanctions that have weakened their supply chains. Although Moscow has produced domestic models such as the Orion, Eleron-3, and Lancet, they have sought out Iran to aid in their drone production efforts. Russia has purchased many Iranian Shaheed-136 drones, which can precisely target stationary

The Drone War:

A Look Into the Impact of UAVs in the Russia-Ukraine War

ground targets carrying 100 pounds of explosives. However, their effectiveness comes with a hefty price-tag, as the Russian government paid USD 193,000 per unit back in November 2022.

During the first year of the war, Ukraine had traditional military air defense systems, which could detect incoming aircraft. To overburden these systems, Russia changed their tactics and launched drones with missiles at high rates, leading to confusion and miscalculation of the radar systems. To combat this issue, Ukraine once again looked to the private sector for help through miltech startups. In this instance, the startup Zvook was brought in to solve this problem and assist drone radar systems. Zvook, an acoustics detection innovator, has repurposed its machine learning capabilities to detect Russian drones, as well as much larger targets such as cruise missiles and fighter jets. Zvook's precision-radar technology has aided the Ukrainian military system's blindspots when detecting aerial activity.

A New Frontier of Warfare

As troop movements on the ground become more stagnant in the war's third winter, the Ukrainian skies have never been more tactically imperative. In early February of this year, Ukrainian President Volodymyr Zelenskyy announced the creation of a new military branch devoted to drones, the Unmanned Systems Force. Military leaders around the world are closely watching this move, which could reshape military management structures to facilitate more coordinated drone efforts and an army built for the future.

In Eastern Ukraine, the drone war is in full force, with two distinct strategies from each military. The Ukrainians have heavily explored the private sector, using commercial drones and startup talent to devise a more innovative and dynamic drone army. Russia on the other hand, has increased domestic drone production and has stockpiled more traditional, military drones, relying on attempts to exhaust Ukrainian capabilities through sheer power and quantity. The dynamic evolution of drone technology witnessed in the Russia-Ukraine War indicates significant implications for the future landscape of warfare. As smaller, agile, and modifiable drones demonstrate their efficacy, militaries globally are compelled to reassess traditional paradigms. This transformative trend signals a shift toward more adaptable and innovative defense strategies. It suggests a future battlefield characterized by innovative tactics and the increasing prevalence of the integration of civilian technology in real-time. Such developments herald a new era in which agility and ingenuity stand as the cornerstones of military preparedness and effectiveness.

By Andrew McKay. Edited by Cameron Vrckovnik.

Narratives of Oppression:

Settler Colonialism in Global Contexts

By Autry Johnson. Edited by Olivia Paul

Narratives of Oppression:

Settler Colonialism in Global Contexts

In 2007, 148 countries attending the United Nations General Assembly 61st session approved a new landmark recognition of Human Rights—the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Four countries abstained: Canada, the United States of America, New Zealand, and Australia. These four countries and Israel all have one common factor: settler colonialism. Their founding fathers are from elsewhere in the world.

Founded after World War II, the U.N. falls short of one of its primary goals: decolonization. Post-war Europe, recovering from fascist regimes and the biggest genocide in human history, saw the West's battlefields shift to the developing world. Israel became the first project for the new Security Council to bring forward a new era of human rights. Israel has the right to exist and remember its history, but to what degree will it protect its own citizens without redoing the injustices of the past?

The parallels between Palestine and the First Nations are striking. In his work "Behind the Trail of Broken Treaties," American Indian Movement (AIM) founder and activist Vine Deloria Jr. emphasized the legitimacy of historical claims to a specific territory as a sovereign heritage. While Israel's claim is valid internationally on the basis of historical claims, Indigenous nationhood is not.

Palestinians have endured the most extensive hypocritical form of sovereignty by settler colonial governments. The USA and Canada do not recognize Palestinian sovereignty. Historical claims to specific territory as sovereign heritage are valid in the context of Israel, yet are not to other the Indigenous nations of the world.

Although UNDRIP is a landmark recognition of Indigenous rights, it is not binding in the corpus juris of domestic states. It is worth bearing in mind that within the Universal Declaration of Human Rights (UDHR) and UNDRIP's language, there is no specific definition of "Indigenous". As a result, the hypocritical viewpoint on Indigenous sovereignty becomes favoured by the hegemonic settler-colonizers throughout the world. In the USA and Canada, Indigenous peoples exist and have the right to "self-determination", although these rights are limited to what their federal governments grant them. The same is true for Palestine; however, its sovereignty is controlled by settler colonialism and in its infancy compared to that of its Indigenous counterparts on Turtle Island.

Although the narrative "Indigeneity" is contested in the Levant on religious grounds, Palestinians face the same persecution Indigenous peoples do. To some parts of the world, they are a people persecuted under a hegemonic government, expelled from their homelands because of insurgents fighting. To others, they are misunderstood and vilified as terrorists. This narrative is nothing new to Indigenous peoples. In the USA and Canada, the tactics of protest control were recently noted during the 2016 Dakota Access Pipeline Protests for sovereignty and land protection, where members acting as water

Narratives of Oppression:

Settler Colonialism in Global Contexts

protectors were labelled "terrorists" by the US. This label was then used to justify the government's use of military tactics against protestors .

Across the sea, the systems of Israeli apartheid and separation mirror the reservation systems in the USA and Canada and the policies they used for the removal of the "Indian Problem" starting in the 19th century.

The portrayal of Indigenous people as "terrorists" fighting for their land serves as a political agenda in the domestic politics of settler-colonialism. The expansion and illegal annexation of lands exacerbated by broken treaties uses this narrative to justify such means. For example, in the USA in 2011, the conviction of Yemeni citizen Ali Hamza—charged for crimes associated with al-Qaeda—used these narratives. US Pentagon lawyer Edward S. White upheld a precedent from the early 19th century during the time of the "Indian Wars," writing that: "Not only was the Seminole belligerency unlawful, but, much like the modern-day al-Qaeda, the very way in which the Seminoles waged war against U.S. targets itself violates the customs and usages of war."

White was challenged for using a racist precedent; however, the US upheld the precedent during the conviction by the Pentagon's general counsel.

As a result of this colonial legacy, peace in the USA took on the form of genocide to culture and people. The federal government created reservation systems to contain the masses, and people needed a laissez-faire pass to leave their confinements. Starvation took the lives of thousands, and those who left the reservations were outlaws and renegades to be criminally hunted down. The Residential School era assimilated Indigenous cultures, and it was illegal to practice their cultures and religions or even to speak native languages. In 2024, Palestine mirrors this fate, and just like their Indigenous counterparts on Turtle Island, the public is divided today on the humanity of actions taken by the Israeli and other settler governments.

Israel is violating many forms of international law, but its right to exist is backed by the settler-colonial governments of the USA and Canada. Israel also wields policies and tactics that settler-colonial governments used to deal with their "Indigenous" population for their nation's security. This is the danger of how hegemonic powers frame their Indigenous problem. If this is peace to settler colonizers, what exactly does it entail for Palestinians and Indigenous peoples?

For centuries in the USA and Canada, the status quo of domestic politics ignored or denied the genocide against its Indigenous population. It wasn't until 2015 that Canada accepted the atrocities of genocide on Indigenous people that were carried out under the false guise of "peace." The USA still has yet to formally recognize these actions. For Palestine, there appears to be little Western recognition, and peace seems to only look like destruction. To move forward toward peace,

Narratives of Oppression:

Settler Colonialism in Global Contexts

the world needs to accept the magnitude of the devastation that colonialism brought and continues to bring to all people.

By Autry Johnson. Edited by Olivia Paul.

Unraveling China's Propaganda Web:

Impact on Taiwan's Elections and the Taiwan Strait Conflict

By Maria Fernanda de Almeida. Edited by Avana Mohandesi

Unravelling China's Propaganda Web:

Impact on Taiwan's Elections and the Taiwan Strait Conflict

Taiwan's recent presidential election in January this year saw William Lai, the Democratic Progressive Party (DPP) candidate, emerge as the victor. The electoral period was characterized by chaotic interference, allowing both China and Taiwan to influence public opinion and reset the confrontational atmosphere across the Taiwan Strait. As Chinese influence campaigns penetrate Taiwan's media battlefield, the question arises: how do strategically orchestrated narratives organized by Beijing affect political outcomes and public opinion in Taiwan, particularly in the aftermath of the recent presidential election? Moreover, how could China's deliberately false information campaigns influence Taiwan's global reputation and impede the pursuit of a peaceful settlement in the volatile Taiwan Strait? This article disentangles the core of widespread Chinese propaganda narratives by investigating its nuances of disinformation campaigns, editorial control, and margin of trust. It shows how the Chinese government has affected the democratic processes, international relations, and the balance of power between Beijing and Taipei.

In the run-up to the election, Beijing engaged in information manipulation using a myriad of tactics designed to sway opinion in Taiwan and the Chinese mainland. This included direct and indirect influences, such as financial operations and disinformation operations, to push for declarations in Taiwan that aligned with Chinese interests of discrediting the Democratic Progressive Party (DDP) and undermining Taiwan's defence capabilities. One of the most classic examples is the manipulation of media ownership. The Taiwanese media conglomerate Want Want Group received subsidies in China and re-injected funds into its media platform in Taiwan. China also reports engaging in 'paid news' deals with Taiwanese media groups in return for introducing more favourable stories on the mainland. Insider reports revealed that Chinese authorities had allegedly paid at least five Taiwan media organizations for coverage across a range of publications and on a television channel.

Regarding disinformation operations, it has been challenging to track the sources behind this indirect influence. Chinese actors have been accused of creating and disseminating false narratives to undermine U.S.-Taiwan relations and manipulate public perceptions. Taiwanese non-state actors have been used to perpetuate narratives that play into existing pre-established social divisions and conspiracy theories within Taiwan's domestic media landscape, distorting the island state's perception, politics, and international relations. Chinese actors have intervened in and exploited the narratives they knew would find a more loyal ear, further weakening the resilience of the domestic media landscape and fuelling domestic conflicts and insecurities, thus endangering the health of Taiwan's liberal democracy and its relations with other states.

Furthermore, China spent billions of dollars to build an information infrastructure to circulate propaganda, censor the internet, and spread disinformation worldwide. The Chinese

Unravelling China's Propaganda Web:

Impact on Taiwan's Elections and the Taiwan Strait Conflict

sets the stage for a conflict less conducive to dialogue and negotiation between Taiwan and mainland China. Besides affecting the arbitration process and Taiwan's appearance on the global stage, China's systematic disinformation campaigns can also have longer-term ramifications. The weaponization of disinformation, whether used to influence elections or divide public opinion, threatens the stability of the Asia-Pacific region and the integrity of the democratic process in Taiwan.

By Maria Fernanda de Almeida. Edited by Avana Mohandesi

How to Fund a Revolution in 2024:

Rebels in Myanmar and the New Age of Armed Struggle

By Napas Thein. Edited by Cameron Vrckovnik

How to Fund a Revolution in 2024:

Rebels in Myanmar and the New Age of Armed Struggle

A civil war has been raging in Myanmar. The country's military junta, which seized power in a coup enacted in February 2021, has been fighting against both newly formed and longstanding resistance forces. Chief among the new pro-democracy actors is the National Unity Government (NUG) with its military arm known as the People's Defence Forces. Alongside them are various decades old Ethnic Revolutionary Organizations (EROs) spread throughout the country. These resistance forces enjoy local and popular support against the widely unpopular junta.

After three years of war, estimates suggest that the conflict has killed more than 50,000 people, internally displaced over 1.95 million, and led to thousands of refugees pouring into neighbouring countries. This conflict further exacerbated the previously ongoing Rohingya crisis and pre-existing internal tensions, including the conflict between various EROs and the central government which constitutes the world's longest ongoing civil war.

However, the tides of the war are shifting. Despite military air superiority, the junta has seen again and again battlefield losses, defections, and surrenders while opposition forces gain significant territorial advances, albeit mostly in rural areas. Some opposition-reported claims suggest that approximately 60 to 70 percent of land in Myanmar was "regained" by anti-junta forces.

But how have these opposition forces, operating with a far lower financial and bureaucratic capacity, managed to muster up enough resources to greatly weaken the ruling military junta?

Myanmar's Diaspora-Powered Crowdfunded Revolution

Like many other countries around the world, Myanmar's people are part of a large international diaspora network located in nearly every megacity from Tokyo to New York. Diaspora-led fundraising efforts, much of it composed of small donations, have made funding both the pro-democracy NUG and various EROs possible.

In pure numbers, the NUG managed to raise over USD 150 million using a variety of financial tools. Fundraising tactics used by the National Unity Government range from the "auctioning" of military-owned property and land (assuming victory in the revolution), the sale of gem mining rights, the offering of "revolution" bonds, and the creation of a cryptocurrency "neobank". Many of the "consumers" of these products are diaspora members in rich nations around the world who are personally invested in on-the-ground outcomes in Myanmar.

Can this sort of crowdfunded warfare translate into real state control and recognition on the world stage?

Theory of War-Making State Power

Scholar Charles Tilly said that "war made the state and the state made war". While his theory has its

How to Fund a Revolution in 2024:

Rebels in Myanmar and the New Age of Armed Struggle

critiques, it provides some points of analysis for evaluating the potential success of grassroots pro-democracy forces. Tilly argued that state-making—the ability of a people to formulate a functioning state—requires the ability to develop a "means of war". This includes the building up of armies and weapons and the ability to generate the money to pay for them. In essence, candidates for statehood had to show that they could not only wage war, but fund it as well.

Historically, states that could take advantage of a large rural population, market economies, and business activity were the ones that could establish strong militaries and win. These were the states, Tilly argued, that became the strong nations in Europe.

Taking Tilly's theory and applying it to Myanmar comes with several issues. Firstly, Myanmar is not a European nation and the environment in which it operates is largely different from that of the European State. Secondly, Myanmar as a "nation" in our analysis is not fighting an external force, but an internal one.

That said, the theory provides some areas of worthwhile reflection. Viewing the situation in Myanmar as a civil war amongst, between, and across actors, we can see how the status and abilities of the actors might determine war outcomes and the development of a new state.

NUG and PDF Crowdfunding as War- and State-Making Revenue Generation

For one, anti-junta actors like the National Unity Government and its allies are participating in a complex—but effective—system of revenue generation. These organizations manage to extract resources from the global diaspora and effectively the global economy. Although perhaps not as reliable as income taxes or customs taxes, this type of revenue generation is raising serious money that is being used to fund revolutionary activity.

The money seems to be working in innovative ways. After only two years, the National Unity Government managed to grow a People's Defence Force from an idea to multiple forces with over 65,000 fighters, not even including the strength of the Ethnic Revolutionary Organizations. This contrasts with the junta's reported remaining 70,000 combat soldiers.

The money is also seemingly going towards "new" makeshift warfare technology. Consumer-level drones-turned weapons have been used throughout the country with the capacity to spy on, carry out airstrikes against, and scare enemy troops. Rebels are adopting techniques and tools to develop 3D-printed guns, unexpectedly with support from Second Amendment-loving far-right groups in the United States and Europe.

How to Fund a Revolution in 2024:

Rebels in Myanmar and the New Age of Armed Struggle

A Civil War with Geopolitical Implications

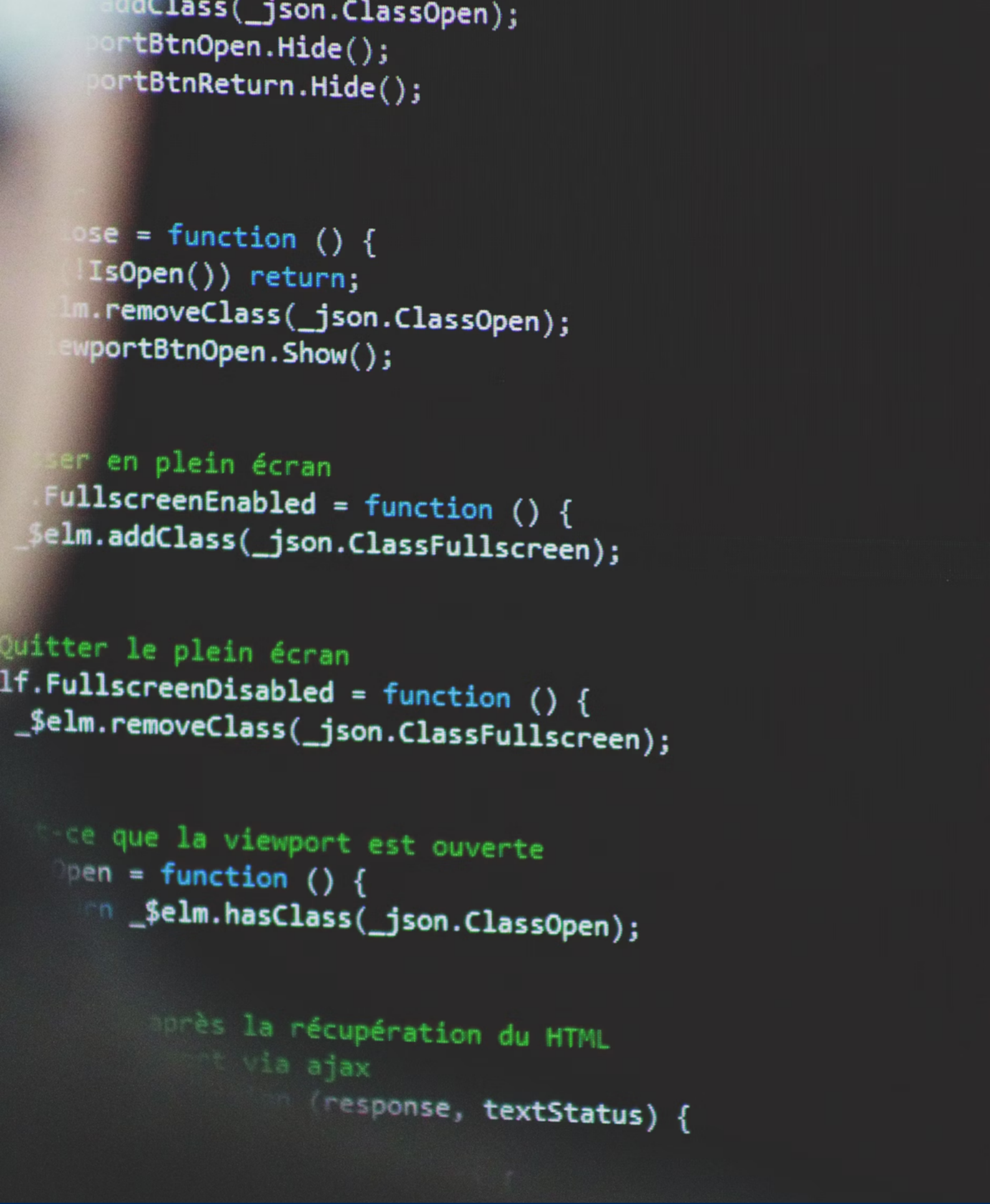
Beyond that, the anti-junta forces are fighting a war that reflects larger geopolitical cleavages. Russia's obvious support for the junta amidst their invasion of Ukraine should be seen, if not already, as a threat point to the West. It is clearly partially an ideological war between democracy and authoritarianism, but it lacks symbolically equivalent support on the democratic side.

Myanmar's case, historically, is rather unique. The country is incredibly diverse, with over 135 major ethnic groups throughout. Its history of democracy, isolated military dictatorship, Japanese and British colonization, and monarchy are embedded in the political psyche of the nation, distinguishing it from its neighbours in China, India, and Thailand. The idea of state development in Myanmar is complex and we should recognize that these new actors possibly will be the next government following the end of the war.

The Weakening Junta

The fracturing of the military junta's power is becoming apparent. They have faced major losses throughout—including a successful offensive by the opposition Three Brotherhoods Alliance—while experiencing major internal turmoil to the point of experiencing over 14,000 defections. Recently, they issued an announcement of mandatory military service for young people throughout the country, a signal of desperation and wavering internal weakness. While timelines remain unclear, the fall of the junta seems to be on the horizon. Innovative crowdfunding, grassroots organizing, and makeshift warfare are the bedrock of this revolution, sparking hope for a new democratic state.

By Napas Thein. Edited by Cameron Vrckovnik



Ransomware Attacks:

A Pressing Threat to State Security

By Sarah Afiane. Edited by Avana Mohandesi

Ransomware Attacks:

A Pressing Threat to State Security

With the growing use of technology and internet systems, it is not shocking that cyberattacks have grown in prominence as global occurrences. Most modern cyberattacks involve some type of malware —"malicious software". Malware attacks are any software code or computer program designed to harm computer systems or their users. These attacks come in various forms, including ransomware, Trojan horses, viruses, and spyware. Cybercriminals develop and use malware for many different reasons, the most common ones including:

1. Holding devices, data, or entire enterprise networks hostage for large sums of money;
2. Gaining unauthorized access to sensitive data or digital assets;
3. Stealing login credentials, credit card numbers, intellectual property, or other valuable information; and
4. Disrupting critical systems that businesses and government agencies rely on.

Although malware attacks are becoming increasingly common, ransomware in particular has taken the lead and raises significant national security risks. Ransomware attacks are a subcategory of malware CISA defines as: "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

This form of cyberattack takes place in various ways, including through exploitation of vulnerabilities, as well as social engineering tactics, such as 'phishing'—emails intended to deceive employees within an organization to open attachments which launch the malware that then infects their networks. Once deployed, the malware software connects to a command-and-control server to enable the criminals to move laterally across networks and encrypt and/or exfiltrate the organization's data.

These attacks have been increasingly used to target state infrastructure and institutions, including businesses, schools, governments, and hospitals. For instance, in 2019, a ransomware attack shut down the operations of a U.S. Coast Guard facility for 30 hours. In February 2020, a ransomware attack on a natural gas pipeline operator halted operations for two days. Further, in October 2021, the health care system in Newfoundland and Labrador was hit with a ransomware attack that caused an IT outage affecting 10 percent of patients in the province and costing the system CAD 16 million. Not only were operations strained for months in the height of the pandemic, but the attack also resulted in data breaches. Specifically, the personal information of over 58,000 patients was obtained, as well as some patients' banking information and SIN numbers.

These cyberattacks on hospitals are troubling as they undermine hospitals' efforts to care for patients, leading to longer hospital stays, delayed tests and procedures, complications from medical

Ransomware Attacks:

A Pressing Threat to State Security

procedures, and even an increased likelihood of patient death rates in some cases. In addition to the harm ransomware attacks have the potential to inflict on critical state infrastructure, they also result in considerable economic impacts on targeted countries. Ransoms paid by private firms amount to millions of dollars toward criminal enterprises every year. The total amount paid by ransomware victims globally increased by 311% in 2020 from 2019, costing nearly USD 350 million worth of cryptocurrency. In Canada, the average cost of a ransomware attack was more than CAD 1.1 million in 2023 compared to CAD 458,247 in 2021—a 150% increase in just two years.

Cybersecurity Attacks can also Undermine Governments

Beyond the more immediate threats posed by these attacks on countries through infrastructure disruptions, data breaches, and economic loss, there is an additional level of threat posed by ransomware: the potential undermining of government. In many cases, the public perceives the government as the primary safeguard against cyber attacks on crucial systems and institutions. While this is common perception, the reality is far more complex, with private companies, software developers, and individuals all contributing to defending against these attacks. However, when institutions are targeted, the public tends to start questioning the government's ability to handle cyber threats, sometimes causing mistrust and a decreased confidence in their government. This political impact can occur either intentionally—as when attackers aim to induce fear and undermine confidence in governments (cyber-terrorism)—or inadvertently as a result of other objectives, such as pursuing economic gain. Regardless of the intent, the risk of undermining governments poses a threat to state security.

Due to the growing prominence of ransomware attacks, there has been increasing international efforts to take down these cyber gangs—such as the recent take down of Lockbit. LockBit, a notorious cybercrime gang, hacks some of the world's largest organizations by stealing sensitive data and threatening to leak it if victims fail to pay an extortionate ransom. In February 2024, Lockbit's operations were disrupted in a rare international law enforcement operation by Britain's National Crime Agency, the U.S. Federal Bureau of Investigation, Europol and Canadian authorities.

Despite this example of international cooperation in the takedown of Lockbit, many ransom hacking gangs remain. As such, it will be imperative for governments around the world to not only prepare for these attacks at the national level, but also aim to work collectively to handle these attacks more effectively.