THE PHILOSOPHY OF CYBER DIPLOMACY. HOW DOES SOCIETY MITIGATE CYBER CONFLICT THROUGH CYBER DIPLOMACY?

Pachara NARIPTHAPHAN
National Broadcasting and Telecommunications Commission, Bangkok, Thailand
Pachara.n@nbtc.go.th

Abstract: The world has entered the age of cyber warfare, where digital devices can jeopardize the livelihoods of human beings and disrupt the stability of nation-states. Nations have undergone digital transformations, leading to a drastic change in the way governments interact. It is imperative to establish effective strategies in order to handle cyber conflicts and shape the future of global diplomacy by fostering trust in cyber technology. The new generation of government officers must develop new skills, with the support of dynamic public policies, to tackle emerging challenges. This includes the realm of diplomacy, which serves as the foundation for cultivating trust. Diplomatic activities play a crucial role in mitigating conflicts, reducing hostile reactions, fostering understanding, promoting dialogue and minimizing interference. However, the evolving cyber landscape necessitates the modification of long-standing diplomatic paradigms, particularly as the current practices seem to be failing the global community. This presents an opportunity to construct a new framework that incorporates cyber diplomacy.
Keywords: Conflict, Negotiation, Technological supremacy, Trust, Trust development, Cybersecurity, Cybercrime, Public policy, National security, Geopolitics, Thailand.

INTRODUCTION

This paper starts with a quick introduction to Thailand's digital landscape. Thailand has undergone drastic changes with digital transformation following the COVID-19 pandemic. The government and the private sector have worked harmoniously to introduce a digital transformation framework in almost every sector of the country. This transformation has been made possible due to a solid foundation in both conventional and digital infrastructure. Additionally, in 2018, Thailand introduced 5G licenses on the market (Phoonphongphiphat, 2020), which has allowed for exponential growth in the capital gains of operators. This aligns well with the government's initiative of "Government 4.0", which began in 2018. The government has established bureaucratic structures aimed at supporting this significant shift towards digitalization. However, there have been some roadblocks in its implementation due to the average age of the government cabinet, which is over 70 years old. Nevertheless, the COVID-19 pandemic has acted as a stimulus, propelling Thailand's EDGI index from 73rd in 2018 to 55th in 2022 (EDGI, 2022). Numerous private and public digital services have been activated, reshaping the economic landscape, while also introducing new threats. The rapid pace of development has outpaced the capabilities of the old security regime. Combined with the global shortage of cybersecurity manpower, the dynamic evolution of unconventional threats has hindered the government's ability to adapt and develop effective policies to counter the growing security risks.

This is indeed a global trend where nations lack capable policing, turning digitization policies into vulnerable targets for security attacks. Core infrastructures, including telecommunications, public health and financial sectors, have become heavily digitized and are facing significant targeting. Both individual citizens navigating these services and the services themselves are subject to collateral damage and targeted attacks. The dimension of these attacks is ambiguous, and the actors involved are often elusive. Nation-state actors, crime syndicates and individual adversaries can carry out similar attacks with comparable effects. Many of these actors intersect with one another. While the understanding of the landscape is still rudimentary, the framework is clear. The impacts are segmented based on the intentions behind the attacks, whether it be for financial gain or destabilization of the target.

While the intentions behind cyberattacks and conventional attacks may be similar, involving damage and theft, it is impractical to treat them merely as variations of each other. This undefined landscape calls for a new definition and necessitates a new set of talents and engagement strategies, along with a new subset of diplomatic theories. This is why the philosophy of cyber diplomacy is explored. This innovative diplomatic framework revises the centuries-old engagement practices of nation-states. The framework is no longer based solely on asymmetry among countries, such as population size or economic strength. The cyber landscape is not constrained by the traditional rules of basic scarcity. It has leveled the playing field, enabling smaller actors like Estonia, Romania, Taiwan and Singapore to operate at the same capacity level as larger G7 countries.

BACKGROUND

It is crucial to understand the fundamental landscape in the paradigm of cybersecurity, which consists of three key landscapes: information, data assets and critical infrastructure. These landscapes form the theoretical foundation of a nation's digital ecosystem.

The information landscape can be initiated as a starting point. The importance of cyber warfare became evident during the Arab Spring in 2010 (Brown et al., 2012). The way digital devices facilitated connectivity among people and encouraged collective action was witnessed. This marked the advent of the first cyber warfare paradigm, which replaced traditional information warfare operations through broadcasting or news media outlets. Not long ago, Al Jazeera served as a tool to shape the hearts and minds of Arabic viewers. The 2010s marked the beginning of a digital transformation when telecommunication technology reached ubiquitous LTE speeds. Credit must be given to Steve Jobs for introducing the personal screen device known as the iPhone to the average consumer in 2007. This device fundamentally changed human-technology interactions, shifting communication from auditory to audio-visual with visual interfaces. It opened up new frontiers in interactive communication technology.

This era gave rise to Zuckerberg's social media, which revolutionized how humans interact and network. Human socialization became dependent on screens connected through telecommunication networks powered by electricity. Niall Ferguson's theory of Square and Tower provides insights into human networking (Ferguson, 2018). However, the aim of this paper is to incorporate technological symmetry into his theory, where the Square represents

the power grid and the Tower symbolizes cellular network towers. Ferguson's theory will be revisited later on.

Information operations, known as I/O, have long been recognized as strategic actions for psychological warfare. They were first introduced during World War I when pamphlets were dropped on villages to terrorize residents, demoralize soldiers, or interfere with military operations. The introduction of personalized digital social media platforms revolutionized modern-day I/O. The Arab Spring served as clear evidence of the impact such platforms can have, and I/O has become increasingly associated with social media rather than conventional leaflet drops or broadcasting media.

Nation-states are adopting new tactics in utilizing social media for their I/O operations. Some countries have even banned social media platforms from operating within their territories. In some cases, nations may design their infrastructure so as to isolate their citizens from accessing unsolicited information disseminated through I/O operations by their adversaries. China, for example, has implemented the Great Firewall to intercept unsolicited or unauthorized services from operating within their closely guarded republic (Wang, 2020).

In 2016, the growing propagation of fake news and deepfakes for I/O purposes was witnessed (West, 2017). The introduction of artificial intelligence and machine learning (AI/ML) has opened new frontiers in I/O capabilities, offering endless possibilities for innovative scams. It is crucial to recognize the global threat posed by scams, as scammers utilize misinformation to deceive victims. The criminal supply chain involved in scams ranges from human trafficking to illegal SIM card and bank account registrations and money laundering. Thai police reported approximately 160,000 local scam cases during a nine-month period in 2022 (Tortermvasana et al., 2023). Arrested scammers revealed that they targeted not only Thai victims but also elderly Americans across the Pacific (Associated Press, 2023).

According to a confidential report received from the International Justice Mission, there is a cross-border operation in the Golden Triangle region involving Thailand, Myanmar and Laos. This operation includes trafficking humans to work in call centers, where well-educated individuals from around the world are deceived into working on Myanmar's territory. Reports indicate that individuals from the Philippines, Uganda, Nigeria and Kosovo were arrested and declared persona non grata after being dumped at the western border of Thailand. The International Justice Mission operates in Thailand to assist trafficking victims worldwide. The report also highlights the illegal call centers exploiting the extrajudicial use of telecommunication infrastructure in Thailand's signal overlapping areas.

The second landscape concerns data assets, and the devastating impact of data breaches on nation-states has been witnessed. The case of WikiLeaks serves as a prime example (Welna, 2019). Julian Assange, a former National Security Agency operative, gained control of massive amounts of information from the US intelligence community. This incident had a tremendous impact on the credibility of the US government in the global community. The WikiLeaks incident highlights the severity of damage caused by digital espionage. Data storage vulnerabilities have become new targets for the intelligence community, combining

signal intelligence (SIGNIT) and human intelligence (HUMINT) to gain access to data and its storage facilities connected through digital infrastructure networks. The acquisition of such data becomes an intelligence asset, acting as both a means and mode of attack.

When used as a mode of attack, leaked data can have severe consequences for national security. The WikiLeaks data, for example, severely disrupted the HUMINT network within the intelligence community. The data breach from the 2015 US Office of Personnel Management exposed significant risks to personnel (Barrett et al., 2015). The same applies to corporate espionage, where leaked data, as it can be seen in the Panama Papers incident in 2016, has political and financial implications (Ryle, 2023). The leaked data undeniably becomes a major risk landscape, with international consequences. For instance, when the WikiLeaks documents presented analytical transcripts on the King of Thailand and the German head of state, the perpetrators found the consequences satisfying and spread the information.

Numerous policies have been implemented to "patch" and protect against future attacks, but the risk continues to increase exponentially. In a recent incident, US National Guard Airmen were arrested for leaking Pentagon documents, which posed alarming challenges in creating policies to protect data infrastructure (Wendling, 2023).

The third landscape pertains to critical infrastructure. As digital transformation progresses, digital infrastructures are expanding their footprint. With financial systems, communication networks and public health services racing to digitize, their increased digital presence poses vulnerabilities. An example of the threat landscape for critical infrastructure can be seen in the 2022 movie "The Operation Fortune" ((IMDb, 2023). The plot revolves around start-up billionaires attempting to purchase stolen AI-based algorithm hacking devices to attack the global financial system and destabilize the central banking systems, leading to the collapse of fiat currencies and disrupting the gold supply. The expectation is to cause a small glitch in the global central banking system that would undermine currency credibility.

More realistic examples include ransomware attacks on hospital systems, where patient records are held ransom for a fee. Such attacks have occurred in Thailand, although many of them have not been publicized due to sensitivity regarding the credibility of the facilities involved (Reuter Staff, 2020). Awareness exists regarding the techniques used by Israeli intelligence to target Iranian nuclear fusion facilities, as it was seen in the Stuxnet attack. This demonstrates how digital equipment can be vulnerable to cyber-attacks, even with air-gap designs. These attacks are designed to disrupt the operations of the targets, which can be nations, organizations, or even individuals. Disruptions to critical infrastructure have catastrophic consequences. A country without electricity or a home without power both experience significant hardships. Similarly, a country without internet connectivity or a person without his communication devices faces significant challenges.

Many nations are forced to digitize their critical infrastructure without the ability to adequately protect it in the cyber realm. As the author of this paper mentioned during the 5th annual Critical Infrastructure Protection Forum in Bucharest, Romania (Naripthaphan, 2022), the Electricity Generating Authority of Thailand (EGAT), responsible for the country's

600Kva power grid, faced twenty attacks in a week. While the attacks were intercepted, the agency was unable to identify the perpetrators. Another common exploitation of power grids is cryptocurrency mining. Likewise, scam call centers exploit telecommunication infrastructure. These exploitations are challenging to prevent because the legal frameworks are insufficient to deter criminals. An adequate international enforcement framework is currently lacking, making it difficult to prosecute and extradite criminals in the virtual and extraterritorial environment.

The three identified landscapes mentioned above form the basis for a new approach to power dynamics, which is meant to be evaluated in order to develop a framework for cyber diplomacy. The tactics employed by attackers, including information operations, data exploitation, and disruptions to critical infrastructure, pose a threat to national stability. These actions have the potential to shift power dynamics and create a polarization of power between actors. Traditional asymmetrical size becomes less significant in this context. It is crucial to explore the concept of power within inter-state relationships in order to establish a diplomatic framework. By understanding and addressing power dynamics in the cyber realm, a more effective navigation and shaping of diplomatic strategies can be achieved.

POWER PARITY

Familiarity exists with the analysis of power dynamics in international relations, emphasizing the traditional understanding of power based on military capabilities and the concept of soft power as defined by Nye (2004). In the conventional paradigm, military power was considered hard power, enabling countries to assert dominance through physical force. The United States differentiated itself from the Soviet Union by effectively utilizing soft power, which encompassed economic and cultural influence. Soft power, as Nye describes it, can yield similar effects to hard power without the need for physical coercion (Nye, 2004).

The United States' cultural and economic power, exemplified by Hollywood and the global dominance of the US dollar, has played a significant role in its global influence. However, the emergence of new challengers, such as Korea and India in the entertainment industry and the rise of the Chinese renminbi as a potential global currency, is reshaping the global status quo. Technological superiority has also been a crucial factor in power dynamics. During the Cold War, the competition between the US and the USSR extended to the space industry, with the US asserting dominance through powerful rockets and advanced physics.

In the present era, the line between hard and soft power has become blurred as technology plays a central role. The advent of digital and virtual operations has introduced a new form of language and weaponry, making cyberspace an arena for power projection and conflict. The development of digital weapons and the ability to conduct operations in the virtual realm have redefined the concept of arms and expanded the scope of power dynamics.

It is essential in highlighting the transformative impact of digitization and technology on the conventional understanding of soft power and hard power. The emergence of the cyber landscape and digital weapons has blurred the lines between these concepts, as technology

now has the capacity to disrupt and influence society, military operations and economic systems. The Arab Spring serves as a prime example of how social media was weaponized to mobilize and coordinate movements, fundamentally altering the dynamics of conflict. Similarly, terrorist organizations like ISIS were able to leverage social media platforms to recruit new members, communicate and sustain their operations. This is how the power parity shifted against the gargantuan nations. The smaller nations can cost-effectively operate in the digital space as opposed to the physical landscape. This can be highlighted through the contemporary conflicts, such as the Ukraine-Russia conflict, as the digital battlefield has become increasingly prominent. Technology has enabled asymmetrical forces to challenge and neutralize conventional military might. Precision drones, satellite communication and cyber penetrations have been utilized to disrupt command and control systems, thereby reducing the disparity of forces.

The significance of size and traditional military capabilities is being reevaluated in this digital era. Ukraine, for instance, was not expected to deter Russia's military strength, yet with the support of advanced technology from the Western world, they were able to level the playing field and effectively resist Russian aggression. Technologies have introduced new forms of leverage, empowering smaller actors and enabling them to confront larger adversaries.

The digitization of warfare and the utilization of advanced technologies have fundamentally altered the dynamics of power and conflict, challenging traditional notions of power projection and military superiority. The ability to harness technology effectively has become a critical factor in contemporary global conflicts.

CONFLICT PHILOSOPHY

A comprehensive overview of conflict is available, ranging from intra-personal to inter-personal conflicts and beyond. Conflict is indeed a pervasive aspect of human civilization, and it exists in various contexts and scales.

The Morton Deutsch International Center for Cooperation and Conflict Resolution (MD-ICCCR) at Columbia University has made significant contributions to the study of conflict. By categorizing conflicts based on forms, needs, politics and faces, they have provided a framework for understanding and addressing conflicts systematically. Professor Peter T. Coleman's work on defragmenting conflicts through protocol-based platforms has been particularly noteworthy in promoting effective conflict resolution strategies (Coleman et al., 2010).

It's important to note that while many conflicts can be resolved through negotiation and diplomacy, a small percentage of conflicts become protracted and difficult to resolve (Coleman, 2011). The Ukrainian-Russian conflict serves as one such case study, which has been closely monitored by organizations like MD-ICCCR. Experts, including individuals like Dr. Pascal De Rocha, who have worked on conflict resolution at the United Nations, provide valuable insights into these complex conflicts. When conflicts escalate to a larger scale, they often involve cultural, linguistic, ethnic, economic and power dynamics. These factors can

contribute to the intensification of conflicts and result in human casualties and suffering. Understanding the various dimensions and causes of conflict is crucial for developing effective strategies to prevent, manage and resolve conflicts in order to promote peace and cooperation among individuals, communities and nations.

An important aspect of conflict was highlighted: communication styles. Dr. Mitchell R. Hammer's work on International Conflict Style, particularly the quadratic matrixes, provides insights into different communication styles used in conflicts. The dichotomy of avoidance and directness in communication has been a significant factor in human conflicts throughout history.

However, the emergence of the digital landscape and the cyber world brings about a new dimension to conflicts. Unlike territorial and cultural conflicts, the cyber world has no physical boundaries, which poses new challenges on moral and ethical grounds. Many existing norms and understandings may not be directly applicable to this new technological conflict paradigm.

Technological advancements such as Artificial Intelligence/Machine Learning (AI/ML), the Metaverse, code and spectrum allocation further complicate the conflict landscape. Concerns are arising regarding the potential dominance of AI/ML technologies over humans, the ethical implications of the Metaverse, and the need for governance frameworks in these realms. Issues such as digital trade frameworks and cybersecurity also come into play as the world adapts to the evolving technological landscape.

The race for technological advancements, such as the ownership of standards for technologies like WiFi7, introduces additional complexities to the conflict landscape. It is evident that new norms and understandings must be developed to effectively navigate and address conflicts arising from these technological advancements.

Efforts are already underway, such as the development of digital frameworks and cybersecurity measures, to address the challenges posed by technological conflicts. However, as technology continues to advance, it is important for societies, organizations and governments to adapt and establish appropriate governance structures, ethical guidelines and legal frameworks to ensure the responsible and beneficial use of these technologies.

As the future unfolds, it will be crucial to continually reassess and adapt the approaches to conflict resolution and governance in the context of the evolving technological landscape.

It is a valid point that the evolving conflicts and challenges in the cyber landscape require a new framework for diplomacy. Traditional diplomacy, as it was mentioned, has often involved a small group of elites representing state interests. However, the digital age has brought about a more interconnected and inclusive world where the voices of various stakeholders, including individuals, organizations and even non-state actors, play a significant role.

Cyber diplomacy, also known as digital diplomacy or e-diplomacy, recognizes the need to adapt diplomatic practices to the realities of the cyber landscape. It encompasses the use of digital technologies and platforms to facilitate diplomatic interactions, negotiations and

resolutions in cyberspace. Cyber diplomacy recognizes that issues such as cybersecurity, data privacy, digital trade and internet governance have become central to international relations.

One of the key aspects of cyber diplomacy is its inclusive nature. It allows for broader participation and engagement, involving not only traditional diplomatic channels but also non-governmental organizations, civil society, academia and the private sector. This inclusivity ensures a more comprehensive understanding of the complex challenges and perspectives in the cyber domain. Cyber diplomacy also requires the development of new norms, rules and frameworks to govern behavior and resolve conflicts in cyberspace. This involves establishing international agreements, conventions and protocols that address issues such as cybercrime, state-sponsored cyber-attacks, norms of responsible state behavior in cyberspace, and the protection of critical infrastructure. Efforts are already underway at various international forums, such as the United Nations, to promote cyber diplomacy and foster dialogue among states and other stakeholders. These initiatives aim to build trust, enhance cooperation and develop shared understandings in addressing the challenges and risks associated with the cyber landscape.

Overall, cyber diplomacy offers a new approach that acknowledges the unique features and complexities of the digital world. By embracing this framework, the international community can work towards a more inclusive, collaborative and effective approach to conflict resolution, governance and cooperation in the cyber domain.

DIPLOMACY

An important point was brought up about the historical development of diplomacy and its focus on state-level interactions. Diplomatic relationships have traditionally been formal, protocol-driven and primarily conducted by elites representing the interests of their respective nations. These interactions often involve exchanges of gifts, visits between leaders and negotiations to establish alliances or resolve conflicts. In the context of cyber diplomacy, there is a need to consider the changing dynamics of the digital world and how they impact traditional notions of diplomacy. While the formalities and protocols of traditional diplomacy may not directly translate to the cyber domain, the underlying principles of diplomacy, such as communication, negotiation and cooperation, remain relevant.

The incentive for cyber diplomatic relationships lies in the shared goals and interests of nations, communities and societies in the digital realm. The digital world has become increasingly interconnected, and the actions of one nation or actor can have widespread implications. Therefore, it is in the interest of all stakeholders to foster peaceful and cooperative relationships in cyberspace.

Cyber diplomacy can play a crucial role in addressing various challenges and promoting positive outcomes in the digital domain. It can focus on issues such as cybersecurity, data protection, internet governance, digital trade and cross-border cooperation. By engaging in cyber diplomacy, nations can establish norms, rules and agreements that enhance security, promote stability, and protect the rights and interests of individuals and communities in cyberspace.

Additionally, cyber diplomacy can facilitate dialogue and collaboration between governments, civil society organizations, academia and the private sector. This broader participation and engagement can help generate innovative solutions, build trust and foster understanding among different stakeholders in addressing the complex issues of the digital world.

While the formalities and structures of cyber diplomacy may still be evolving, the underlying objective remains the same: to establish connections, promote cooperation and create a peaceful and harmonious digital community. By embracing cyber diplomacy, nations can work together to navigate the challenges and opportunities of the digital age while upholding the principles of diplomacy and fostering a positive digital environment for all.

A point was made about the power of networks and connectivity in shaping the modern world, as discussed by Niall Ferguson (2018) in "The Square and the Tower". The emergence of digital platforms, such as social media, has indeed transformed the way people connect and communicate across the globe. These platforms have created hubs and spokes of information and interaction, allowing individuals to connect based on shared ideas, ideologies, identities, objectives and needs.

Ferguson's analysis showcases how historical examples, such as the influence of masonic lodges and the Arab Spring, demonstrate the power of networks in driving societal change. The impact of digital platforms on social and political movements, as seen in events like the Arab Spring, demonstrates the ability of these networks to facilitate widespread mobilization and coordination without the need for physical interactions. The platforms amplify the impact of social and political movements. The rise of TikTok as a platform for user-generated content and its influence on elections in Thailand further exemplify the power of these networks to shape public opinion and drive engagement. The resonance algorithm and visibility on platforms like TikTok play a significant role in shaping information delivery. The rising prominence of visual and audible platforms has transformed how information is consumed and shared. It thus aggrandizes competition against more traditional forms of political messaging.

In the realm of cyber diplomacy, the pace of connectivity and resonance within these networks becomes crucial. The ability to quickly disseminate information, connect with diverse stakeholders and resonate with audiences at a large scale is vital in shaping diplomatic efforts in the digital age. Algorithms and AI matching play a significant role in enhancing visibility and facilitating network connections, allowing cyber diplomacy to operate at an accelerated pace.

To effectively engage in cyber diplomacy, diplomats and policymakers must recognize the power of these networks and leverage digital platforms to establish connections, promote dialogue and shape narratives. Understanding the dynamics of information delivery, psychological resonation and network connections becomes essential in navigating the fast-paced and interconnected landscape of the digital world.

By harnessing the potential of digital networks and employing strategic approaches to cyber diplomacy, policymakers can leverage the power of connectivity to foster understanding, build relationships and address global challenges in a more inclusive and efficient manner.

Within this context, cyber diplomacy must operate at the pace set by these digital networks. The ability to connect, resonate and disseminate information quickly and effectively becomes crucial. The use of AI matching and hub-based networks allows for large-scale and rapid connections within these digital platforms, shaping the landscape in which cyber diplomacy takes place. In the realm of cyber diplomacy, it is important for diplomats and policymakers to understand the dynamics of networked communication, psychological resonation and algorithmic visibility. By leveraging these insights, policymakers can adapt their strategies to engage with audiences, foster dialogue and address global challenges in the interconnected digital world. The crucial role of networks in diplomatic engagement was noticed, encompassing both formal and informal relationships. Building connections and fostering relationships, with both allies and adversaries, is an essential aspect of diplomacy. These networks often include back-channel channels or informal channels that enable discreet and confidential communication.

The rapid pace of digital network connections in the information landscape presents a significant challenge for traditional diplomatic practices. The speed at which information spreads through digital campaigns and user-generated content can potentially lead to inter-governmental conflicts. The mentioned example, the US-China panda fiasco, illustrates how user-generated content on social media platforms can quickly penetrate networks, breaking diplomatic barriers and challenging established protocols. It becomes challenging for governments to keep up with public sentiment, even in highly controlled environments like China. The open nature of social media platforms means that once information is released, it can be challenging to control or contain its spread.

An important point was raised regarding data security as the second landscape in the context of cyber diplomacy. Data breaches and attacks aimed at discrediting or targeting national state actors have had significant diplomatic implications. The case of Edward Snowden and the subsequent WikiLeaks disclosures demonstrated the challenges of maintaining data security and the potential impact on diplomatic relations. The situation surrounding Julian Assange and his residency in the Ecuadorian embassy in London further highlighted the complex diplomatic issues that can arise from data leaks.

In order to address data security and protect national and private data assets, collaboration and collective efforts are essential. A framework for cyber diplomacy should prioritize the establishment of a community that promotes awareness, shared responsibilities and accountability. Cross-functional protection measures, such as the Red Hat approach, which involves a collaborative and open-source approach to security, can be valuable components of this framework. By working together and sharing best practices, nations can enhance their data security and mitigate the risks associated with cyber threats.

The third landscape of cyber diplomacy, as exemplified by large-scale cyber security attacks in countries like Albania, Costa Rica and Ukraine, highlights the need for new forms of private-public diplomatic partnerships. These attacks have demonstrated that government efforts alone may be insufficient to effectively respond to and recover from such incidents. As mentioned by Hoffman (2023), there is a requirement for enhanced capacity building at the local level to ensure effective resilience.

The existing international legal framework may fall short in deterring and addressing cyber perpetrators due to challenges in enforcement. To establish effective reciprocity in digital assistance, it is crucial to develop mechanisms that facilitate the provision of foreign digital assistance at the state level. This requires a well-designed framework that places emphasis on competency building and shared responsibility. The traditional reliance and parenting models in diplomacy may no longer be suitable in the context of cyber threats. Instead, a competency-building approach, as demonstrated by the success of the Ukrainian digital force, can be a valuable model. By focusing on enhancing competencies and skills, countries can develop their own capabilities and foster collaborative partnerships with other nations to address cyber security challenges effectively.

An important aspect of diplomatic frameworks was highlighted, which is the building of trust. Trust can be categorized into two major components: identification-based trust (IBT) and calculus-based trust (CBT), as discussed by Lewicki and Tomlinson (2010). IBT is based on shared interests and common topics, while CBT is rooted in common strategic goals. IBT tends to be more sustainable, but it may not always be feasible due to varying national interests. Both IBT and CBT play a role in diplomatic relationships. In the context of digital diplomacy, interests are often different from traditional diplomatic interests. Digital interests intersect private and public domains, necessitating broader interactions and the use of egalitarian platform systems. When interests are shared by a larger community, it becomes easier to create representation of diplomatic interests, facilitating meaningful relationships and collaboration.

By leveraging network connections and the convergence of digital interests, diplomatic frameworks can foster trust-building processes that involve both IBT and CBT. These frameworks can enable effective engagement and cooperation between nations, facilitating the resolution of shared challenges and the pursuit of common goals in the digital realm.

The author participated in the 2nd Cyber Diplomacy conference in Bucharest, Romania, this event being an excellent example of a digital diplomatic initiative. Such conferences provide a platform for connectivity among networks of shared digital interests, allowing smaller nations to have a more relevant role in the global community. The aim is to develop the mechanics of cyber diplomacy and create larger-scale network connectivity through technology and digital platforms, where expertise can be shared.

This approach represents the second generation of diplomacy, an upgrade achieved through human scientific achievements. It encompasses various diplomatic relationships, including C to C (civil society to civil society), B to C (business to civil society), G to G (government to government), C to G (civil society to government) and B to G (business to government). These relationships form a strong foundation for engagement and cooperation.

The example provided of the connection between Hong Kong's umbrella movement and Thailand's three fingers movement illustrates how C to C cyber diplomacy can transcend physical boundaries and create shared interests or IBT through network connections. Building alliances of this nature is crucial in cyber diplomacy, with a focus on the technological landscape, rather than solely the political one. The technological and scientific communities often have strong alliances and the ability to achieve and maintain both IBT and CBT.

The International Telecommunication Union (ITU) is another example of diplomatic collaboration in the technological realm. As an organization that predates the formation of the United Nations, the ITU is respected and trusted by nations, exemplifying CBT. Collaboration through organizations like the ITU is essential in managing the complexities of the digital landscape and fostering trust among nations.

Cyber diplomacy should be based on a decentralized and egalitarian framework, fostering strong cross-interaction between citizens (C), organizations (B) and governments (G). Trust-building should be a central focus, both at the calculus-based trust (CBT) and identification-based trust (IBT) levels. The framework should also be dynamic and flexible, adapting to the rapidly evolving cyber landscape. Here are the following guidelines for the framework:

1. The framework must be built on an egalitarian model, taking into account the decentralized nature of digital network platforms. Even in centralized nations like China, equal access and opportunities should be provided to both private and public entities to participate in the platform;

2. Community policing is essential within the framework. Every member should share the responsibility and duty to police the community, protecting each other from potential adversaries;

3. The framework should include a public archive of digital tools and digital weapons, ensuring transparency and accountability in the cyber domain;

4. Shared capacity should be emphasized within the framework. Cross-organizational assistance and collaboration should be promoted, while adhering to appropriate rules and guidelines;

5. Encouraging the use of open-source software infrastructure (OSS) is important, as it empowers the community and builds trust among participants without the ambiguity of commercial interests;

6. The hardware infrastructure of the framework should be based on an open platform model, with dedicated common spectrum to ensure availability of access. This dedicated spectrum and frequency should be protected by the community police to maintain connectivity assurance;

7. The framework should encourage technological neutrality and be unbiased. The technology utilized should prioritize human-centric approaches, taking into consideration the needs and interests of individuals.

Small nations benefited from these frameworks by equalizing the size and economic leverage of the bigger nations. The decentralization will enforce the egalitarian ideology of the framework. Preparing for the cyber diplomacy platform, it is important to acknowledge that conventional government systems are also attempting to issue multiple frameworks. For instance, the US has its digital trade framework, Russia has its treaty on cybercrime, and the EU has its cyber resilience system. While these frameworks have their advantages and disadvantages, they are often structured according to old bureaucratic mindsets and can

be laborious. They lack the dynamic structure required for the digital era, which presents a conundrum.

The question arises: should the US lead all the current frameworks and initiatives? Is the conventional legislative and foreign affairs approach capable of handling the new threat landscape? Furthermore, does the current hegemonic system, led by the US, create more conflicts in our polarized world?

The author emphasizes the need for a framework that is decentralized and egalitarian because that is how the world should operate in the digital age. It provides an opportunity for smaller countries to have a voice and contribute to the balancing of global policies. This is how the second-generation diplomacy should function.

MOVING FORWARD

It is crucial for the cyber diplomacy framework to have an egalitarian approach, as fixating on the status quo would ultimately lead to failure. The emergence of the cyber world has brought about a new paradigm in terms of armament, weaponry and strike capabilities. The efficiency with which countries like Iran and North Korea operate in the digital realm has been noticed. The digital world has shifted the traditional power dynamics, giving smaller nations a bigger voice in the global community.

However, it is important to acknowledge that larger nations have certain advantages in terms of resources and capabilities, while smaller nations are still in the process of building up their capacities. In an effort to lead cyber diplomacy, the United States is working towards establishing a space and cyber bureau within the framework. The US government is focusing on advocating for digital freedom and human rights. Liesyle Franz, who was part of the US's cyber diplomacy initiatives in the early 2000s and participated in the development of the first internet framework policy, highlights the importance of recognizing these changes and adapting to them.

The US's efforts will help smaller nations understand the significance of capacity building and achieving independence in the global cyber ecosystem. Given the ongoing reliance on corporate platforms and software, it is essential to recognize the limitations and effectively manage their use, allowing nations to retain control over their cyber status.

To address the challenge posed by large corporations in the digital realm, it is important to acknowledge the issue of the digital divide. Just as the Second Amendment in the United States guarantees the right to bear arms, in the digital world, individuals should have an undeniable right to access technology and devices. It is crucial for governments to adopt a "no one left behind" approach, ensuring that all individuals have access to the necessary tools and resources to participate in the digital world.

Cyber diplomacy will play a significant role in making this a reality. It will help governments understand and navigate the complex ecosystem that underpins the functioning of the digital world. By promoting inclusivity and equal access to technology, cyber diplomacy can work towards narrowing the digital divide and ensuring that individuals have the opportunity to fully participate in the digital age.

CONCLUSION

The author of this paper shares the hope that cyber diplomacy becomes more than just a concept and evolves into a practical reality. It is indeed crucial to establish mechanisms that support global collaboration and enable effective communication in the digital age. Language, or lingua franca, plays a vital role in diplomacy as it facilitates communication and connection between different stakeholders.

To build a platform for cyber diplomacy, the focus must be directed on three fundamental elements: information, data assets and critical infrastructure. These elements have been exploited by adversaries to target and disrupt systems, emphasizing the need for collaboration to prevent such exploitation and ensure peace and harmony.

Conventional diplomacy alone is insufficient in the digital era, where economic, social and security paradigms have shifted significantly and discrepancies have been reduced. This is where cyber diplomacy comes into play. By adopting a framework that emphasizes decentralization and an egalitarian model, access and communication is guaranteed for all stakeholders, overcoming the limitations of traditional diplomatic etiquette.

Addressing the issue of the digital divide and promoting capacity building are essential steps in realizing cyber diplomacy. It has the potential to become a social innovation and should be adopted globally to foster collaboration, secure communication, and navigate the challenges of the digital world effectively.

REFERENCE LIST

Associated Press. (23 March 2023) *Thai police bust call scammers who swindled older Americans*. NBC News. https://www.nbcnews.com/news/amp/rcna76271.

Barret, D., Yardon, D. & Paletta, D. (5 June 2015) U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.

Barone, M. (2004) *Hard America, Soft America: Competition vs. Coddling and the Battle for the Nation's Future.* US, Crown Forum Publisher.

Brown, H., Guskin, E. & Mitchell, A. (28 November 2012) The Role of Social Media in the Arab Uprisings. *Pew Research Center*. https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/.

Chulov, M. (11 April 2021) Israel appears to confirm cyberattack on Iran nuclear facility. *The Guardian*. https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility.

Coleman, P. T. (2011) *The Five Percent: Finding Solutions to Seemingly Impossible Conflict.* New York, USA, PublicAffairs Publisher.

Coleman, P. T., Deutsch, M. & Marcus, E. C. (eds.) (2010) *The Handbook of Conflict Resolution*. 3rd ed. New Jersey, USA, Jossey-Bass – Wiley Publisher.

EDGI. (2022) *UN E-Government Knowledgebase*. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/169-Thailand/dataYear/2022.

Ferguson, N. (2018) *The Square and the Tower: Networks and Power, from the Freemasons to Facebook*. London, UK, Penguin Press.

Gan, N. & Wang, S. (2023) "Bring Ya Ya Home': How a panda in the US turbocharged Chinese nationalist sentiment. *CNN*. https://edition.cnn.com/2023/04/26/china/china-us-ya-ya-panda-diplomacy-intl-hnk/index.html.

Hoffman, D. (2023) *The Future of Cyber Security policy*. United States Telecommunication Training Institute. https://ustti.org/wp-content/uploads/2023/05/Cybersecurity-by-David-Hoffman.pdf.

IMDb. (2023) *Operation Fortune: Ruse de Guerre*. https://www.imdb.com/title/tt7985704/.

National Aeronautics and Space Administration – NASA. (29 October 2013). *The Decision to Go to the Moon: President John F. Kennedy's May 25, 1961 Speech before a Joint Session of Congress*. NASA History Office, DC. https://history.nasa.gov/moondec.html.

Nye, J. S. (2004) *Soft Power: The Means to Success in World Politics*. New York, USA, PublicAffairs Publisher.

Phoonphongphiphat, A. (20 May 2020) Thailand leads Asian in 5G rollout due to pandemic. *Nikkei Asia*. https://asia.nikkei.com/Spotlight/5G-networks/Thailand-leads-ASEAN-in-5G-rollout-due-to-pandemic.

Reuter Staff. (10 September 2020) Thai hospitals and companies hit by ransomware attacks. *Reuters.* https://www.reuters.com/article/us-thailand-hospital-ransomware/thai-hospitals-and-companies-hit-by-ransomware-attacks-idUSKBN2611WV.

Ryle, G. (2023) Ten years of exposing the financial secrets of some of the world's most powerful people. *The International Consortium of Investigative Journalists*. https://www.icij.org/investigations/offshore/ten-years-exposing-offshore-tax-havens-secrets/.

Tortermvasana, K., Leesa-Nguansuk, S. Kasemsuk, N. & Banchongduang, S. (6 February 2023) Online scammers in the crosshairs. *Bangkok Post*. https://www.bangkokpost.com/business/2499931/online-scammers-in-the-crosshairs.

Wang, Y. (1 September 2020) In China, the 'Great Firewall' Is Changing a Generation. *Politico.* https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385.

Welna, D. (11 April 2019) 12 Years of Disruption: A WikiLeaks Timeline. *National Public Radio (NPR).* https://www.npr.org/2019/04/11/712306713/12-years-of-disruption-a-wikileaks-timeline.

Wendling, M. (14 April 2023) Jack Teixeira: National Guard airman arrested over leaked Pentagon documents. *BBC*. https://www.bbc.com/news/world-us-canada-65269975.

West, D. M. (18 December 2017) How to combat fake news and disinformation. *Brookings*. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

Yang, W. (22 November 2020) Thai inspired by Hongkong protest movement. *Deutsche Welle*. https://www.dw.com/en/thailand-hong-kong-protests/a-55373873.

Pachara NARIPTHAPHAN

Is currently an Executive Advisor to the Chairman of the National Broadcasting and Telecommunications Commission for the Royal Thai Government. His responsibilities include supervising and overseeing international affairs, external affairs and academic affairs of the Office of National Broadcasting and Telecommunications Commission. He has extensive experience as a political manager, having managed ministerial offices at the Ministry of Energy, Ministry of Finance, Ministry of Industry, Ministry of National Resources and Environment and Ministry of Information and Communication Technology. He was awarded a scholarship for a doctoral degree in biology from Shanghai Jiaotong University by the Chinese government. He obtained his Master's Degrees from Columbia University and Boston University, and his Bachelor's Degree from University of Southern California. Prior to his appointment at the NBTC office, he served as an advisor and researcher at the Centre of Global Challenges, at the Asia Institute of Technology. He was also an executive committee member of the Puea Thai Party, where he was responsible for economic and digital policy. In addition, he has significant experience as an instructor in transformational and ethical leadership, family relationships, political communication and change management.