Establishing Effective Cyber Diplomacy and Deterrence Capabilities Between International Partners

Cristian-Vlad OANCEA
Provision IT Group, Bucharest, Romania
vlad.oancea@protonmail.ch

Abstract

Changes has been always a constant in a modern and dynamic world, but the rapidity of change in the global security landscape accelerated after 9/11 and global war against terrorism. There is a new approach regarding political, ideological, economic and military race due to globalization which improved the landscape with good practices and developmental growth but is still a major driver of instability. While threat of conventional decrease, accordingly the spread of conflict, it complexity, accuracy, changeable and reach into many areas have emerged. Many new types of warfare have also emerging like cyber, network, digital, information, economic, media pursued cross domains both in peace or war. Especially nowadays but also during challenging times, deterrence has been an important part of foreign affairs of a nation, to conserve internal and external stability and preserve its integrity.

Index terms: Cyber Diplomacy, Cybersecurity, Deterrence, IoT

1. Introduction

The etymology of "deterrence" starts with the Latin word "deterre" – to frighten from or away. The dictionary defines deterrence as "the action that persuades an opponent to give up something that is desired." [1]

Deterrence discourages an opponent from pursuing an unwanted action. It is a complex subject guided by a number of types, theories, forms, strategies and many other factors. All countries are managing and expanding their strategic area to secure freedom to conduct multi-domain actions by a wise combination of creating alliances and increasing their comprehensive national power which leads to an increased level of deterrence capability.

Deterrence requires a national strategy that integrates diplomatic, informational, military, and economic powers. India must develop strategies, plans, and operations that are tailored to the perceptions, values, and interests of specific adversaries. Deterrence strategies and actions must be developed for all phases of confrontation and conflict planning. Deterrence operations must, therefore, be planned and executed across all domains in concert with other elements of national and international power in order to achieve strategic objectives. A crucial aspect is that successful deterrence is knowledge-dependent and requires the ability to establish and secure communication access to adversaries in order to generate the desired decision outcomes. Human intelligence (HUMINT) naturally is essential in seeking to understand an opponent's values, culture, decisions, risk and capacity for situational awareness as well as obtaining other information required for effective deterrence. Situational awareness is the sine qua non for deterrence where political direction,

intelligence community, diplomacy, law enforcement, military, and even economic inputs must get synergised. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence. Effective deterrence combines military and non- military means. In some cases, military capabilities may not be an effective tool to deter a particular adversary's action, making other instruments of power the primary deterrent. Additionally, the support of strategic partners should be integrated to increase deterrence credibility, but deterrence must be applicable as a unilateral approach. The deterrence will obviously be challenged by other affected Nations. Military actions will always remain the final pivotal option to achieve national objectives both proactive and reactive. One very important factor which is being increasingly accepted is the mind of the leader and people and their likely reaction to deterrence. I would like to re-emphasize here, that deterrence in security parlance covers a very wide spectrum of activities and domains and not just employment of armed forces.

2. Enhancing inter-operability between NATO and EU Member States

The major interest nowadays is to expand cooperation in fields that will support the realisation of objectives that NATO and EU Member States and organisations share. The EU Member States and NATO are capable of complementing each other well. Examples include the "PESCO" project [1] and the Multinational Medical Coordination Centre in Koblenz, Germany. A project for the storage of medical equipment tools was developed under the responsibility of the European Medical Command and the related agency is already in use.

This point highlight that the enhanced cooperation between NATO and the EU Member States is important for the nations that are not part of both organisations at the same time. The breakthrough regarding the participation of non-EU nations in PESCO that was negotiated under the German Council Presidency and will help further expand cooperation and thereby further improve the existing operational result.

Strengthening Europe's possibility to act, in this case, does not constitute a weakening of NATO nor does it question NATO, which is works well and serves its scope. An enhanced cooperation serves to improve both organisations ability to act. After all, this represents a shared goal: to improve an ability to act to guarantee future security for and in Europe.

3. Moving toward a unified interpretation of cyber operations within the Law of Armed Conflict

Security culture in the information age presents a lot of challenges. The cyber revolution gives get up to new threats and opportunities requiring immediate actions and policy responses. Understanding its nature and especially the consequences for security represents a slow learning process. Interpretation of cyber fact involves analysis of a new body of experience that actual existing assumptions may be unable to clarify. It requires a technical understanding of a changing technology, whose implications require time to learn and analyze because of its scientific complexity. The result has been a delay in the strategic reshaping to cyber actuality. The contemporary world faces up to an enormous cyber threat. The U.S. intelligence community rates this threat higher than global terrorism and warns of the potential for a catastrophic cyberattack. The range of feasible cyber conflicts is poorly understood by students or decision makers and it is quite unsure how conventional security mechanisms, such as deterrence and collective defense, apply to this fact. In addition, the principles of cyber offense and cyber defense still remain essential.

Also, the rules of engagement (ROEs) [2] for cyberspace operations have received increasing attention as opportunities for achieving military objectives in and through cyberspace have become more feasible. To the scope probable, it is necessary to apply the same principles that government the use of kinetic weapons to the use of cyber weapons, while recognizing the special attributes of the cyber space and cyber weapons. This has demonstrate to be a difficult challenge. A lot of the military's actual capabilities in the cyberspace field and the ROEs correlate to their purpose, still remain classified. Through inference, informed speculation and an growing audience understanding of the elementary technology, a growing shape of unclassified information is available regarding the principles and concepts that guide how decision makers formulate ROEs for operations in cyberspace.

In the kinetic world, proceeding quickly is often necessary to mitigate an immediate threat. Also, similar aspects have been applied to threats in cyberspace. Given the speed with which a cyber threat may cause damage, a reaction may be needed very quickly to mitigate or disrupt it. In fact, the duration on which action is needed may be so short as to prevent human involvement. However, an automated response may lead to unexpected and collateral outcome for which the consequences are not totally understood.

4. Bridging the gap between industry, academia and militaries

The rapid step of digital transformation is changing every aspect of our lives and is also creating needs for new skills and knowledge in the workplace.

Rapid technological evolution is changing the way businesses operate. Emerging and cutting edge technologies such as the Internet of Things (IoT), Cloud computing, Automation or Artificial Intelligence (AI) are enabling new model based, distributed, machine enabled business models and creating extraordinary opportunities to create new value. As job profiles, industry and military field evolve, shortages and mismatches can result, but universities may be able to help.

Private companies, government, the military industry and academia are all taking steps to close the cyber talent gap; however, their existing efforts and traditional approaches may not be sufficient to resolve the issue.

Applying a human-centric lens to the cyberspace ecosystem for cyber talent reveals critical action items that affect every level of the employee life cycle, from creating the overall talent pool and recruiting the right people to onboarding new hires, continuously developing new skills and expertise, retaining top talent, and even offboarding people in a manner that preserve an organization's talent brand.

Emerging technologies such as automation and artificial intelligence should be used to increase the traditional cybersecurity efforts. However, such technologies do not remove the need for human talent.

Governments at all levels play an important role in the cybersecurity talent ecosystem, not only in terms of needing such talent to defend systems and data, but also in terms of initiating policies and programs to support address the talent shortage.

The cyber talent gap definitely represents a global risk; but in coordination between governments, educational institutions, public and private sectors, military area, the cybersecurity talent area can rise and be seen as a leader by making confident moves and changing the face of this actual shortage.

Mastering the cyber talent shortage and addressing cyber risk effectively will require an innovative talent strategy, supported by a solid culture and a basic human and technology infrastructure.

Closing the cyber risk gap and enabling organizations to capture the full promise and importance of new technologies is a great opportunity of our time. Emerging technologies such as AI, Machine learning and Big Data can help expend an organization's traditional cybersecurity efforts; however, all those technologies will not skip the need for human talent, at least, not any time soon.

References

[1]. https://www.britannica.com/topic/deterrence-political-and-military-strategy.
[2]. https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO).
[3]. https://www.readcube.com/articles/10.1093%2Fcybsec%2Ftyx003.