Cyber Compellence: An Instrument of Technology-Driven Strategy

Mohsin Azhar Shah*

Abstract

The core thesis of this article is to establish that technology has an increasingly significant role in strategy and policy formulation. The instrument through which this relationship is examined is Cyber Compellence using the Sony Pictures Entertainment hack as a yardstick to analyse its effectiveness. It is concluded that the impact of cyber technology on governance and policy formulation is rapidly emerging and is likely to become very significant in the near future, hence, a technology-driven and aware culture needs to be promoted.

Key words: Cyber Warfare, Cyber Coercion, Cyber Compellence, Strategy, Technological Determinism, Cybersecurity, Sony Pictures Entertainment.

Introduction

With advancements in technology, civilised nations developed tools and weapons that were primarily meant either to 'get the desired' or to 'deter' unwanted (threats) from others (take for instance, the 'Narrabeen Man' - the first victim of spears). Technology is

* The author is a Lecturer at the Lahore School of Aviation, University of Lahore, Pakistan.

IPRI Journal ▪ XVIII (1): 101-119.

a dual-edged sword holding the potential for progress and destruction at the same time. Apart from analysis of the violent discourse of human behaviour, one analytical approach is to assess the role of technology alone in impacting human thinking and behavioural patterns. If we observe technological developments over the history of mankind, it becomes quite evident that human behavioural patterns have been greatly influenced by the advancements in technology. However, as one of the founders of the Society for the History of Technology, Melvin Kranzberg writes 'technology is neither good, nor bad, nor is it neutral,'[1] - the way it is used is relative.

This article focuses primarily on how Information Technology (IT) can shape decision-making and affect strategy formulation in the international system. In order to explore this broader area of investigation, the author looks at the concept of Cyber Compellence, what the term means, its nature, and to determine how this concept provides a linkage between technology and strategy.

Technological Determinism measures the role of technology in framing particular socio-political and socio-economic patterns. It is a theory or a doctrine which suggests that acts of will, occurrences in nature, or social or psychological phenomena are causally determined by preceding events or natural laws. It is an extension of the concept of Determinism - a philosophical doctrine which assumes that all events occur as a consequence of some necessity, and are therefore, not controlled by will. However, Technological Determinism as adopted for this article may not necessarily be strictly associated with the insignificance of free will. In other words, technology has not been taken as a radical concept in terms of Determinism and admits the role of free 'will' in decision-making and policy formulation processes. 'Invention is the mother of necessity'[2] - the emergence or 'invent' of certain technology has often contributed to the evolution of strategic thought, and thereby, suggests that sometimes the notion of *cause and effect* is reversed.

---

[1] Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws'," *Technology and Culture* 27, no. 3 (1986): 544-560.

[2] Ibid.

The use of cyber means to achieve political ends has been in practice for a few decades now as the United States (US) has been using cyber weapons since the 1990s,[3] yet 2012 has been suggested by Adam Segal as the 'Year Zero' in the timeline of cyber warfare.[4] Thus, the cyber domain may still be considered in its infancy. Although a number of cyber operations have taken place in this nascent cyber age, the case of the Sony Picture Entertainment (SPE) Hack is exclusive in nature as it serves to be an ideal case to study Cyber Compellence in action (maybe for the first time in the true sense of 'compellence'), and as a yardstick to analyse the relevance of Technological Determinism to strategic decision-making and policy formulation.

The Revolution in Military Affairs (RMA) was only conceptualised and actualised after the advent of various technologies - the consequences of which have no precedence at all. A technology-driven RMA has a greater focus on the relatively nascent technologies in terms of strategy. One of the most significant aspects of RMA in this regard is the introduction of 'cyberspace' into the strategic realm resulting in the emergence of cyber warfare. Cyber warfare may, thus, be suggested as *an instrument of technology-driven strategy that contemplates a futuristic battlefield and furthers the evolution of strategy*. In this article, the concept of 'a technology-driven strategy' shall be tested utilising the instrument of cyber warfare by analysing its offensive capabilities and translating them into a Compellence Strategy. Generally, the concept of Cyber Compellence has not been studied exclusively in the existing literature, although it has been discussed to some extent as a subset of Cyber Coercion. This article will, therefore, exclusively focus on this less explored yet significant dimension of Cyber Strategy.

[3] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Manoeuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016).
[4] Ibid.

Technology as a Precursor to Strategy

The practice of formulating state policy on the principles of Technological Determinism is not a new phenomenon. An astute analysis of historically significant strategic developments and the evolution of military strategy reveals that technology has long been playing a defining role in strategy formulation to achieve the political objectives of states (or non-state actors as well). Often, the advent of a new technology may give birth to a certain set of strategies. This claim can be tested by looking into the historical developments in the strategic framework being influenced by the advent of new technologies. The advent of artillery revolutionised old siege warfare by overcoming the safety and security of fortresses, thus rendering them more vulnerable than safe. The concept of countervalue targeting may also find its roots in that era as well. Much later, in Twentieth Century warfare, the advent of mechanised warfare, and later, the utility of aircrafts in war again revolutionised military strategies.[5] Historically, one of the most significant RMA was the dawn of nuclear technology, and more recently used for strategies based on the development of precision-guided munitions. However, a true revolution may be seen developing from the transformation of the battlefield from physical landscapes to virtual or cyberspace. Cyberspace is a product of advancement in technology that has given birth to a whole new canvas of strategic thinking in terms of warfare.

Cyber Warfare: A Paradoxical Term?

Cyber warfare may be described herein as 'the science and art of waging war in cyberspace.' It is important to note that the term 'war' as mentioned in the cyber domain may not necessarily incorporate the brute use of force and violence. Rather, the concept of war as introduced by Carl von Clausewitz makes more sense in cyberspace as far as this study is concerned. Clausewitz described war as the 'continuation of politics by

[5] Sharjeel Rizwan, "Revolution in Military Affairs (RMA)," *Defence Journal* (2000), accessed September 6, 2016, http://www.defencejournal.com/2000/sept/military.htm.

other means.'[6] Thus, cyber warfare utilises cyber means to achieve political ends. One of his most famous observations is that:

> …war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means.[7]

Clausewitz transformed the violence and chaos of warfare into a reasoned tool of political will. Equally important, he clearly outlined that warfare was an act of *compellence*, not unremitting violence. This is such a key proposition that he opens his book with it:

> War is, thus, an act of force to compel our enemy to do our will.[8]

Cyber warfare is a new and complex phenomenon since it apparently lacks certain ethical and moral cosiderations of war, which may include violent means and brute use of force on comparatively larger scales. The issue of attribution is also contested when it comes to cyber operations. However, it may be noted that a cyberattack can have violent and kinetic physical effects, including the destruction of property as has been observed in the case of Stuxnet attack which damaged the centrifuges of the Natanz nuclear facility, and the cyberattack on a German steel mill.[9] Moreover, there are also possibilities of life-threatening cyberattacks like hacking a pacemaker to inflict fatal damage as well.[10]

---

[6] Carl von Clausewitz, *On War*, ed. Michael Eliot Howard and Peter Paret (Princeton: Princeton University Press, 1989).

[7] Ibid.

[8] Michael T. Plehn, "The Sharpest Sword: Compellence, Clausewitz, and Counter-insurgency" (paper, Air War College, Air University, Hoboken, 2005), http://www.dtic.mil/dtic/tr/fulltext/u2/a476995.pdf.

[9] CSIS, "Significant Cyber Incidents" (Washington, D.C.: Center for Strategic and International Studies, 2016), https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity.

[10] James A. Green, ed., *Cyber Warfare: A Multidisciplinary Analysis*, Routledge Studies in Conflict, Security and Technology (London: Routledge, 2015).

The cyberattacks against Estonia and Georgia, and the Stuxnet episode all had political objectives which they served quite effectively. As far as issues associated with difficulties in attribution are concerned, states are often more likely to divert attribution away from themselves, but may at times want to achieve the opposite impact in order to gain effective political leverage[11] which leads to the effective utilisation of the concept of Cyber Compellence. Thus, the term 'Cyber Warfare' can be appropriately used to describe 'war' in cyberspace. The NATO Cooperative Cyber Defence Centre of Excellence defines Cyber Warfare in the US / Russian perspective as:

> …cyberattacks that are authorised by state actors against cyber infrastructure in conjunction with governmental campaign.

The South African definition also suggests a likewise scenario, where:

> Cyber warfare means actions by a nation/state to penetrate another nation's computers and networks for purposes of causing damage or disruption.[12]

However, both of the above mentioned definitions do not incorporate the role of non-state actors in a cyber-conflict; whereas, in the context of realpolitik, nation-states may find it more reasonable to deploy cyber offensive operations within the domain of non-state actors or by using proxy networks.

Aptly recognising the nascent nature of cyber war, Myriam Dunn Cavelty describes it as a 'set of new operational techniques and a new

[11] Neil C. Crowe, "The Attribution of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A. Green, Routledge Studies in Conflict, Technology and Security (London: Routledge, 2015).

[12] CCDCOE, "Cyber Definitions," accessed February 11, 2018 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence), https://ccdcoe.org/cyber-definitions.html.

mode of warfare.'[13] According to her, cyber war is primarily 'a new form of command and control warfare (C2W)'[14], which is suggestive that it is not only a new form of the operationalisation of war, but also a strategic framework that is based on an altogether newer form of operational ground or battlefield - cyberspace. She acknowledges, while elaborating her concept of cyber war, that this kind of war requires more of an 'electronic cyberspace' than a geographical terrain.

Thus, cyber warfare is not a paradoxical term, rather, it is a much more evolved and complex form of warfare. It may be argued that in the present world or in the foreseeable future, cyber warfare is not likely to replace traditional conceptualisations of war and warfare, but it needs to be acknowledged that it has already contributed remarkably in the evolution of strategy and in shaping critical elements of modern warfare. Due to its complex nature, it is difficult to confine cyber warfare to traditional conceptualisations of war and requires an understanding of the environment and battlefield where it can be operationalised. Thus, it is important to comprehend the nature and dynamics of cyberspace among other dimensions of cyber warfare.

Cyberspace

The term 'cyberspace' has been defined in a number of ways. Rebecca Grant describes cyberspace in *Victory in Cyberspace* as '… a single medium, but (it) has multiple theatres of operation.[15] By this definition, Grant acknowledges its complex nature. Martin C. Libicki describes cyberspace in his book *Conquest in Cyberspace*, as 'the sum of the globe's communication links and computational nodes.'[16] This description of cyberspace links it more to the context of information warfare conceptualisation. Another definition in a similar context is given by

[13] Myriam Dunn Cavelty, "Cyberwar," in *The Ashgate Research Companion to Modern Warfare*, eds. George Kassimeris and John Buckley (New York: Ashgate Publishing, 2010), 127.
[14] Ibid.
[15] Rebecca Grant, *Victory in Cyberspace* (Arlington: Air Force Association, 2007).
[16] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007).

Duncan Hodges and Sadie Creese as 'the environment within which electronically mediated communication occurs.'[17] Gregory Rattray in his book, *Strategic Warfare in Cyberspace*, explains that:

> Cyberspace, however, is actually a physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place.[18]

Here the physical elements and infrastructure upon which cyberspace is constructed in being ignored. This may also incorporate subtly the considerations for significant warfighting tactics of disrupting and denying the enemy's access to information and communication by targeting its physical infrastructure including (but not limited to) the undersea cable network connecting the globe, the ground-based stations and servers and the satellites that behold and incorporate the cyber cosmos. The US Department of Defence (DoD) defines cyberspace as:

> ...a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[19]

This definition gives a more detailed description and elaborates its various components, thus, incorporating mobile phones, embedded processors, and controllers etc. in the picture as well. For the purpose of this article, however, cyberspace may be defined as 'a medium where digital or quantum communications and operations may occur.' This definition has been adopted to signify the evolution and advancement of technology, on the one hand, since the broader environment of IT is not just based on electronic architecture; and on the other, it also focuses on

[17] Duncan Hodges and Sadie Creese, "Understanding Cyber Attack," in *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A. Green, Routledge Studies in Conflict, Technology and Security (London: Routledge, 2015).
[18] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: The MIT Press, 2001).
[19] *DOD Dictionary of Military and Associated Terms*, s.v. "cyberspace," August 2017.

the isolated or 'air-gapped networks' where direct communication with the external environment may not be occurring, but digital or quantum 'operations' are being conducted. This also expands the scope of cyberspace from being a subset of IT, where information operations and communications are occurring, to a much broader environment where 'digital and quantum operations and processes' take place in machines ranging from simple embedded processors to complex supercomputers and satellites or any other machines capable of carrying out such tasks.

Cyber Compellence: A Subset of Cyber Coercion

Compellence is a comparatively less discussed category of 'coercion' that is a 'timeless form of dispute resolution.' Coercion includes both the denial and punishment aspects of strategy that may be translated by means of deterrence and compellence, respectively. This article focuses on the punishment aspect of coercive strategy that is subject to the change of *status quo* as demanded by the compellence compared to the deterrence model of a persistent desire for the same. Thomas C. Schelling coined the term 'compellence' to define coercive threat or use of power in order to get an adversary to change behaviour.[20] There are two basic forms of compellence: diplomacy and demonstration. Diplomatic or Immediate Compellence involves verbal threats and promises (show of force also assist this kind of coercion). Realist scholars note that 'most diplomacy is underwritten by the unspoken possibility of military action.'[21] Demonstrative Compellence involves limited use of force coupled with the threat of escalating violence (which may also include a full-scale war to come) if demands are not met.[22] Cyber Compellence may, thus, be defined as:

[20] *Encyclopedia Britannica*, s.v. "compellence," May 30, 2014, https://www.britannica.com/topic/compellence.
[21] Richard J. Samuels, ed., "diplomacy," in *Encyclopedia of United States National Security* (Thousand Oaks: Sage Publications, 2006).
[22] Ibid.

> The demonstration of the cyber capabilities (or cyber power) either actively or passively in a manner so as to force or 'compel' the adversary to change the *status quo*.

The active demonstration of cyber capabilities may refer to the deployment of cyberattacks to compel an adversary towards a desired action. Whereas, passive compellence may infer using diplomatic compellence, i.e. by displaying a capability via establishing strategic cyber command centres *per se*. This includes another factor, that is, passive attack - an indirect manoeuver of deploying cyber force in a fashion similar to irregular warfare. Cyber warfare may very well be addressed as a component of irregular warfare and benefit in a similar fashion as the use of insurgency-based proxy wars. Details of this utilisation of cyber power will be addressed in the next section.

Cyber Compellence is different from traditional concepts related to compellence which is considered a subset of coercion or a means to practice the 'power to hurt' The former does not necessitate the display of capability to inflict physical damage, although it may not exclude any such option either. It may involve all the aspects of a cyber operation, including but not limited to disruption, to inflict physical infrastructure damage, hacking and doxing (i.e. disclosing hacked information). It may also be noted that while cyber warfare, let alone Cyber Compellence, may appear meek compared to conventional or nuclear military means, yet it has the potential to surpass the impacts of brute use of force. The North Korean missile tests and their consequences support this claim. In April 2017, North Korea launched a series of missile tests, however, it has been argued that a missile launch that failed shortly after it was fired may have been thwarted by cyberattacks from the US. It has been suggested by the former British Conservative Foreign Secretary Sir Malcolm Rifkind that:

> The missile tests could have failed as there is a very strong belief that the US - through cyber methods - has been successful on several occasions in interrupting these sorts of tests and making them fail.[23]

[23] Julian Ryall, Nicola Smith and David Millward, "North Korea's Unsuccessful Missile Launch 'May have been Thwarted by US Cyber Attack'," *Telegraph*, April 16, 2017.

The same story was earlier published in *New York Times* by David E. Sanger and William J. Broad as well that reflected similar connotations regarding the failure of DPRK's missile test. In the same article, William J. Perry, Secretary of Defence in the Clinton administration, was quoted as saying 'Disrupting their tests would be a pretty effective way of stopping their ICBM program[me].'[24] This argument seems appropriate given the former US President Barack Obama's 'proportionate response' statements, while reacting to the SPE hack, wherein, he ordered to 'step up' the cyberattack and electronic warfare capabilities particularly to counter the North Korean missile tests.[25] However, on the contrary, it was argued by Jeffrey Lewis that the failure of the North Korean missile launches was not because of any US-based cyber operation, rather a consequence of experimentation of new systems that were not being used by the North Korean regime previously, and because 'rocket science' is not easy.[26] Nonetheless, if the US involvement is proven to disrupt and sabotage Pyongyang's missiles, the domain of cyber operations will exponentially be enhanced and may even challenge the credibility of nuclear deterrence.

Methods and Characteristics of Cyber Compellence

A model for Cyber Compellence must include some explicit 'targets' and some arguably identifiable 'compeller(s)' with definite motives and demands that should be declared explicitly. If there is no explicitly or arguably identifiable compeller, the case may not be declared or considered as one of Cyber Compellence. For instance, the case of

[24] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyber War against North Korean Missiles," *New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

[25] Ibid.

[26] Jeffrey Lewis, "Is the United States Really Blowing Up North Korea's Missiles?" *Foreign Policy*, April 19, 2017, http://foreignpolicy.com/2017/04/19/the-united-states-isnt-hacking-north-koreas-missile-launches/.

Stuxnet attack against Iran's nuclear facility cannot be declared as one since it did not include any explicitly identifiable attacker, neither were there any specified demands by anyone. The case of the SPE hack, however, can be declared a case of Cyber Compellence, and thus, is discussed here. Furthermore, establishing and maintaining strategic cyber command is important for signaling in order to achieve Cyber Compellence. However, it is a way of communicating 'passive' or Diplomatic Compellence as compared to 'active' or Demonstrative Compellence and may be restricted to a bilateral (or multilateral) conflict with distinctive adversaries. Active or Demonstrative compellence refers to the display of Cyber Compellence by using cyberattacks against the target to achieve desired ends. Furthermore, this would be more effective if it has the capability of 'reusability and reversibility', i.e. ability to use the same exploit again and again against the same target within the cyber domain.[27] Reversibility refers to the capability of an attack that can turn the target back to its original status as it was before the attack. This helps in 'controlling' the extent to which damage may be inflicted and also gives an attacker the option to make the target systems reusable again if that suits him/her or them. This reversibility characteristic of a particular cyberattack can play an important role in compellence as the attacker may threaten the adversary by using a cyberattack of low intensity, and after the acknowledgement of the attack by the adversary, the attack may be reversed and attacker may achieve a strong position from where the adversary can be threatened with an attack of greater magnitude, and thus, be compelled to do the desired. A Cyber Compellence model, therefore, may be comprised of the declared (explicit) motives and intentions of compeller(s) that are communicated to the target(s) wherein the credibility of the compeller's capabilities to inflict unacceptable damage should be evident for it to work effectively.

[27] Clinton M. Woods, "Implementing Cyber Coercion" (Masters diss., Naval Postgraduate School, Monterey, 2015), https://calhoun.nps.edu/bitstream/handle/10945/45277/15Mar_Woods_Clinton.pdf.

Why Cyber?

The rationale for the utilisation of cyber warfare as a tool for coercion based on a Compellence Strategy has many dimensions. As Sun Tzu suggests a good strategy is one where the weakest spots of the enemy are targeted, perhaps nothing fits this better than cyber warfare as targeting in cyber operations is done by exploiting the 'zero days' or loopholes in the target's computer networks and systems. Moreover, cyber force provides a more suitable premise for coercion through compellence as it is absolutely in accordance with the philosophy of coercion and does not necessitate the use of brute force. Byman and Waxman suggest that using threats alone without deploying threatening instruments (particularly brute force) is more in line with traditional non-lethal coercion.[28] Cyber force helps achieve the desired outcomes at lower escalation levels, hence, saving the costs of war.

Moreover, since strategy is driven by technology, it is important to become acquainted with relevant progresses in the technological domain at earnest, to avoid any kind of developments that may give space to vulnerabilities. The credibility of the coercive instrument of cyber power requires being prepared to any counter-strike in retaliation to the deployment of cyber weapons. Thus, a successful Compellence Strategy incorporates both offensive and defensive measures. After all, 'if you are in the glass house, you should not be the one initiating throwing rocks at each other.'[29] Col. William D. Bryant of the US Air Force suggests that the attack surface should be reduced by eliminating unnecessary capability in both hardware and software, and resisting users' desire for continued rapid improvements in capability without adequate security testing, and segment their networks and systems into separate enclaves.[30]

---

[28] Ibid.

[29] Gregory Rattary quoted in Ellen Nakashima, "Iran Blamed for Cyber Attacks on U.S. Banks and Companies, *Washington Post*, September 21, 2012, https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.f35cb440d2d6.

[30] William D. Bryant, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* 9, no. 4 (2015): 87-107.

Therefore, enhanced defensive capacity building may be prioritised over the utilisation of unchecked networked operations in order to reduce vulnerabilities. Moreover, the concept of utilising cyber force is already on the 'battlefield' now as evident from a number of cyber-related incidents that at least threaten the strategic stability and *status quo*. Therefore, it is necessary not only to get prepared in terms of cyber defence, but also a greater focus should be on the development of offensive cyber capabilities. The argument for preparing for cyber offensive capabilities may be best explained and supported by the Prisoner's Dilemma model, i.e. a state must acquire the capabilities, before its adversaries do so, in order to achieve the best possible outcomes (by exploiting the vulnerabilities or 'zero days' that might not expire otherwise because of delays). Sooner or later, most states will resort to the offensive utility of cyber power, as would be a rational choice, so the ones stepping into the cyber domain first will benefit most, and others may lose the advantage.

The Sony Pictures Entertainment (SPE) Hack Case

The case of SPE hack provides strong evidence of the use of cyber force allegedly by the proxy of a weaker state against a stakeholder of a much powerful state in a manner so as to inflict comparatively much lower costs to the compeller(s). The SPE is a US entertainment subsidiary of Sony Entertainment Inc., which is a subsidiary of Japanese multinational technology and media conglomerate Sony. On November 24, 2014, SPE was hacked by a North Korean hacker group which identified itself by the name Guardians of Peace (GOP). The GOP hacked SPE using a malware and leaked confidential data and posted employees' personal information and unreleased films online. The attack was, in response to a satire focusing on a plot to assassinate North Korean leader Kim Jong-un, and threatened terrorist attacks at cinemas screening the film. North Korean state-sponsored hackers are suspected by the US of being involved in part due to specific threats made towards Sony and movie theatres showing

The Interview. Moreover, North Korean officials had previously expressed concerns about the film to the United Nations (UN),[31] stating that:

> To allow the production and distribution of such a film on the assassination of an incumbent head of a sovereign state should be regarded as the most undisguised sponsoring of terrorism as well as an act of war.[32]

These official statements preceding the hack indicate the likely involvement of the North Korean state in the hack, and thus, highlight the 'compellor' to an extent.

The threats to Sony were taken seriously in the beginning and the movie was pulled off. However, former US President Barack Obama commented on the hacking and stated that he felt Sony made a mistake in pulling the film, and that the producer should 'not get into a pattern where you are intimidated by these acts.' He also said, 'we will respond proportionally and we will respond in a place and time and manner that we choose',[33] which suggest a retaliatory cyberattack. Two messages (both allegedly from GOP) were released afterwards stating that they would not release any further information if Sony never releases the film and removed its presence from the Internet. The other message stated that the studio had 'suffered enough' and could release *The Interview*, but only if Kim Jong-un's death scene was not 'too happy.'[34] This case presents an

[31] An analysis of the letter by the DPRK's Permanent Representative Ambassador Ja Song Sam to the UN Secretary-General Ban Ki-Moon and the remarks by the US President in Year-End Press Conference explains the phenomena of Cyber Compellence. On June 27, 2014, DPRK's Ambassador expressed concerns in his letter to UN against *The Interview* and suggested the production and distribution of the movie as an 'act of war.'

[32] Martyn Williams, "DPRK Takes 'The Interview' Movie Complaint to the UN," *North Korea Tech*, July 10, 2014, www.northkoreatech.org/2014/07/10/dprk-takes-the-unterview-movie-complait-to-theun/.

[33] Barack Obama, "Remarks by the President in Year-End Press Conference" (speech, Washington, D.C., December 19, 2014), White House, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

[34] Elizabeth Weise, Kevin Johnson and Andrea Mandell, "Obama: Sony 'Did the Wrong Thing' When It Pulled Movie," *USA Today*, December 19, 2014,

example of the success of Cyber Compellence by persuading (or compelling) the target not to take an undesired action, at least for a short period. The attack also demonstrated the potential of offensive cyber capabilities or the potential to use cyber capabilities offensively.

It is interesting to note that neither the perpetrator nor the victim of the attack are 'states', rather non-state actors and even the target organisation is not of US origin, yet the response from the US representatives is reflective of inter-state conflicts, in this case confined within the domain of cyber warfare.

A brief analysis of developments in the international community and states' stance concerning the incorporation of cyberspace into their strategic and technological framework suggests that cyber warfare is a significant instrument of technology-driven strategy and policy. The establishment of strategic cyber command centres by various countries provides an example of policy being derived from technology. Cyber Compellence is the translation of cyber warfare as an instrument of technology-driven strategy. An increase in 'focused' cyberattacks is an indication of increasing reliability of strategic policy formulation upon the technological framework. Offensive postures of strategic cyber commands as established or being established clearly indicate the future of Cyber Compellence as a key instrument of a technology-driven strategy.

Criticism on Cyber Coercion and Compellence

Cyber warfare in itself is a contested concept often considered to be primarily based upon low-level intrusions and attacks of low intensity in terms of the damage inflicted, while, compellence has a less coercive weight with respect to its strategic objectives. However, cyber warfare is evolving rapidly with kinetic cyberattacks having the potential to inflict significant strategic physical damage (as has been observed in the case of Stuxnet).

On the other hand, the capability to target an adversary at its sensitive points makes coercion and compellence more effective;

http://www.usatoday.com/story/news/2014/12/19/sony-the-interview-hackers-gop/20635449/.

however, there remains a risk of an unwanted and maybe a non-proportional retaliatory response by the adversary. For instance, if a cyberattack sabotages or cripples a state's nuclear capability, it will more likely retaliate with all possible options, including the use of brute force against the perpetrator of the attack. Hence, targeting sensitive spots of the adversary, which is a requirement of an effective coercive strategy for compellence, may result in an unwanted escalation of the conflict. Therefore, the dilemma of Cyber Compellence is that its use is undermined if escalation of the conflict is to be avoided. However, the threshold of a cyberattack is much higher than an equivalent kinetic attack, and this can be observed from the historical context as the retaliation to Stuxnet attack did not result in an escalation of conflict in terms of brute use of force.

Last but not least, the issue of difficulty of attribution renders Cyber Compellence a less successful tactic since without demonstrating the identity of the attacker, the advantages of compellence may not be fully achieved. However, as mentioned by Neil C. Crowe, voluntary attributability is desired by states for the effective political utility of cyber warfare.[35] The same is true for the effectiveness of Cyber Compellence, as it is a significant instrument of cyber warfare. Furthermore, an implicit attribution may be sufficient for it to work effectively. A hypothetical scenario has been discussed by Travis Sharp wherein it has been established that Cyber Coercion (or Compellence) may work very well even if the identity of the coercer is not revealed explicitly.[36] Therefore,

[35] Crowe, "The Attribution of Cyber Warfare."

[36] Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony," *Journal of Strategic Studies* 40, no.7 (2017): 1-29. "As a plausible hypothetical, imagine an ongoing international crisis in which a country was killing ethnic minorities. The UN Security Council had passed a resolution condemning the violence. A permanent member of the Security Council engaged in a long-running dispute with the violator had frequently expressed its desire to stop the violence. At this point, a coercer launches an anonymous cyber operation that begins harming the target. Despite lacking a verbal demand, only a truly autistic target would be confused about the coercer's likely identity, the nature of its demand, and the steps required to stop the pain (i.e. stop killing minorities)."

when it comes to the utility of cyber force to compel an adversary, the issue of attribution does not hold much ground.

Conclusion

Since the use of cyber force in the Estonian conflict (2007), Georgia's limited war with Russia (2008) and the Stuxnet attack (2010), the claim that a cyber war will not happen does not hold strength anymore. Cyber warfare is already on the battlefield and it is vital to determine the ways it can be effectively countered in order to develop proper security mechanisms and safeguards. Cyber warfare, being an instrument of a technology-driven strategy, may best be translated using Cyber Compellence which in turn may serve as an effective instrument of a technology-driven policy.

The case of the SPE hack is a vitally significant occurrence in terms of cyber warfare as it provides empirical evidence for the first time to the theorists of 'first and third *movements* in strategic analysis of the cybersecurity,'[37] as Travis Sharp puts it, to study Cyber Compellence exclusively. Since the SPE hack warrants that the latter can be a significant component of strategy and policy formulation, it may be adopted by more and more states as indicated by the establishment of cyber command centres in the West, having offensive postures. Hence, countries adapting to a Cyber Compellence Strategy first are likely to benefit more.

While the study of coercion through cyber power by means of Cyber Compellence is an intellectually tough subject to comprehend, let alone examine, theorising it through the Technological Determinism framework may be a useful lens. This article suggests that dependency on technological advancements, particularly in the cyber domain, has increased manifold in a state's policy formulation process, and this dependence on the latter is expected to exponentially increase in coming decades. It is concluded that the traditional conceptualisation of coercion and compellence is applicable in the cyber domain. However, this application of conventional wisdom is not simple and may require a

[37] Ibid.

number of adjustments in order to have the desired effect. It is, thus, in the interest of a state not only to promote a culture of technology with an apt focus on Research & Development in the cyber domain, but also to develop a technology-oriented political culture that may relatively outweigh technocracy over other modes of governance.■