2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations

Pascal Brangetto
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia
pascal.brangetto@ccdcoe.org

Matthijs A. Veenendaal
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia
matthijs.veenendaal@ccdcoe.org

Abstract: Information Warfare and Influence Operations are, in principle, intended to get your own message across or to prevent your adversary from doing so. However, it is not just about developing a coherent and convincing storyline as it also involves confusing, distracting, dividing, and demoralising the adversary. From that perspective, cyberspace seems to be ideal for conducting such operations that will have disruptive, rather than destructive outcomes.

The means through which influence can be exerted relies mostly on spreading information. However, there are more intrusive ways to influence specific audiences that remain in the information realm but are designed to change, compromise, inject, destroy, or steal information by accessing information systems and networks. This paper aims to tackle the following questions: when does influencing the behaviour of an audience become the primary effect of a cyber operation, and which cyber operations might qualify as such? We introduce the term Influence Cyber Operations (ICOs) to describe these actions in cyberspace.

In order to address these questions, and drawing from existing literature, this paper defines ICOs as a specific subset of Influence Operations. ICOs encompass activities undertaken in cyberspace affecting the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences. To illustrate the case for ICOs, we comment on a broad range of techniques that can be used in order to conduct these, and discuss the accompanying policy frameworks.

Keywords: *influence operations, information operations, information warfare, strategic communications*

1. INTRODUCTION

Nations have always used information to enhance their goals and policies as conflicts have never been limited to the military realm.[1] Today, with its rapid expansion, cyberspace seems to be ideal for conducting Influence Operations, maybe even more than for conducting destructive operations.[2] As Tim Stevens puts it, 'cyber warfare of the future may be less about hacking electrical power grids and more about hacking minds by shaping the environment in which political debate takes place'.[3]

The objective of Influence Operations is predominantly to exert power by influencing the behaviour of a target audience; the ability for 'A to have B doing, to the extent that he can get B to do something that B would not otherwise do'.[4] Influence Operations are thus assumed to modify attitudes and shape opinions through the dissemination of information and conveying of messages.[5] However, there are more intrusive ways to influence a specific audience that remain in the information realm but can no longer be regarded as the application of soft power as they are no longer designed to achieve their objective solely through 'attraction'.[6] Cyberspace offers numerous possibilities for these kinds of coercive operations, which are designed to influence a target audience by changing, compromising, destroying, or stealing information by accessing information systems and networks.

The question then arises: when does influencing the behaviour of an audience become the primary effect of a cyber operation and which cyber operations might qualify as such? This paper addresses this question by describing the cyber aspects of Influence Operations and how their technical features may play an active role regardless of their content. We will therefore focus on the relevance of intrusive cyber operations to Influence Operations, for which we propose the term Influence Cyber Operations (ICO).

In this paper, the authors argue that coercive ICOs will become more prevalent because they offer the opportunity to undermine an opponent's credibility with little risk of escalation. When defining ICOs, we highlight the confusion pertaining to the terminology regarding Influence Operations (Section 2). The main attraction for the use of ICOs lies in the fact that they are generally limited in scope and difficult to attribute, thereby limiting the risks of escalation and countermeasures. This is especially reflected in the Russian approach to Information Warfare, which considers it as an instrument of hard power. By contrast, because of the importance

[1] 'The expansion of the domain of warfare is a necessary consequence of the ever-expanding scope of human activity, and the two are intertwined.' in Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, 1999, p. 189.

[2] 'Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security' Statement of James Clapper for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee, 26 February 2015, p.1 http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf. (All Internet resources were accessed 4 March 2016).

[3] Ben Quinn, 'Revealed: the MoD's secret cyberwarfare programme', *The Guardian*, 16 March 2014, http://www.theguardian.com/uk-news/2014/mar/16/mod-secret-cyberwarfare-programme.

[4] Here, we use the definition provided by Robert Dahl in his seminal article, 'The concept of Power', *Behavioural Science*, 2:3, July 1957.

[5] William Hutchinson, *Influence Operations: Action and Attitude*, 2010. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1032&context=isw.

[6] Joseph Nye, 'Soft Power, the means to succeed in world politics', *Public Affairs* 2004, p. x.

Western democracies attach to issues of legality and transparency, their options for using ICOs remain, in principle, limited. Looking at the different approaches (Section 3), this paper then describes what ICOs look like and how they may be applied (Section 4) and provides conclusions and basic recommendations (Section 5).

2. THE DEFINITION CONUNDRUM

In 2007 Martin C. Libicki noted 'that well over a decade after the topic of information warfare broke out into the open, its conceptual underpinnings remain weak and largely unsatisfactory, with fierce battles raging over neologisms and definitions'.[7] Almost a decade later, progress on this issue remains slow. There is still a lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain. Regarding the use of terms like Information Warfare (IW), Psychological Operations (PSYOPS), Influence Operations (IO), Strategic Communications (STRATCOM), Computer Network Operations (CNO), and Military Deception (MILDEC), there is a lot of confusion as there are numerous conflicting definitions, and these terms are used in different contexts to describe different objectives and actions.[8] When trying to make sense of the information domain it is therefore necessary to clarify and define the terminology that is used in this paper. The authors of this article do not, however, seek to provide any definitive answers on this issue.

The main reason for us to provide specific definitions is that Influence Operations are not limited to military operations, but can be part of any kind of conflict, including, for example, in the diplomatic arena. They are therefore part of a larger effort by nations to exert power over adversaries.

In principle, Influence Operations offer the promise of victory through:

> 'the use of non-military [non-kinetic], means to erode the adversary's willpower, confuse and constrain his decision-making, and undermine his public support, so that victory can be attained without a shot being fired'.[9]

They include all the efforts undertaken by states or any other groups to influence the behaviour of a target audience, in peacetime or during an armed conflict. It is therefore the umbrella term for all operations in the information domain, including all soft power activities. Although Influence Operations are, in principle, non-violent, they can be part of military operations.

In addition, Influence Operations are not solely confined to the application of soft power. They can also include clandestine and intrusive activities undertaken as part of an armed conflict or

[7] Martin Libicki, *Conquest in Cyberspace, National Security and Information Warfare*, 2007, Cambridge University Press, p. 17.

[8] This confusion is underlined by the definition of Information Warfare (IW) provided by RAND in Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston, *Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities*, Rand Corporation, 2009 p 2. 'Information Warfare is conflict or struggle between two or more groups in the information environment' which is such a blanket definition that, although technically correct, it borders on being useless.

[9] Anne Applebaum, Edward Lucas, *Wordplay and War Games*, 19 June 2015, http://www.cepa.org/content/wordplay-and-war-games.

military operation. This is in line with the definition we use in this paper, which includes the possibility of the use of intrusive cyber capabilities:

> 'Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further [a nation's] interests and objectives'.[10]

For the much-used term 'Information Operations', we rely on the US DoD definition, which defines it as a military capability that is:

> '[t]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting [its] own'.[11]

In our approach, Information Operations are therefore a subset of Influence Operations limited to military operations.

If Influence Operations are also understood to include intrusive operations, it becomes necessary to separate the 'apples' of information content from the 'apple carts' of information systems.[12] This is in line with Russian thinking on Information Warfare, which traditionally makes the distinction between 'informational-technical' and 'informational-psychological' activities. The semantic or cognitive actions (apples) consist mainly of attacks of information on information (typically narrative vs narrative) that affects the semantic layer of cyberspace. In other words, these are the activities in cyberspace that aim to produce content to create a crafted informational environment. These content-oriented activities can be defined as Inform & Influence Operations (IIOs) that we define as follows:

> 'Inform & Influence Operations are efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages'.[15]

Strategic communications (STRATCOM) and propaganda activities fall under this category, as well as the deliberate dissemination of disinformation to confuse audiences.

The 'apple carts' of Influence Operations concern the technical actions that target the logical

[10] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston, *Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities*, RAND Corporation, 2009 p. 2.

[11] US Department of Defense, Directive 3600.01. May 2, 2013. p.12.

[12] This comparison is taken from Christopher Paul, *Information Operations, Doctrine and Practice, a Reference Handbook*, Praeger Security International, 2008, p. 37.

[13] Timothy Thomas, *Recasting the Red Star*, Foreign Military Studies Office, Fort Leavensworth 2011, p. 138, http://fmso.leavenworth.army.mil/documents/RecastingRedStar_2015.pdf.

[14] See Martin Libicki, *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge University Press, pp. 24-25.

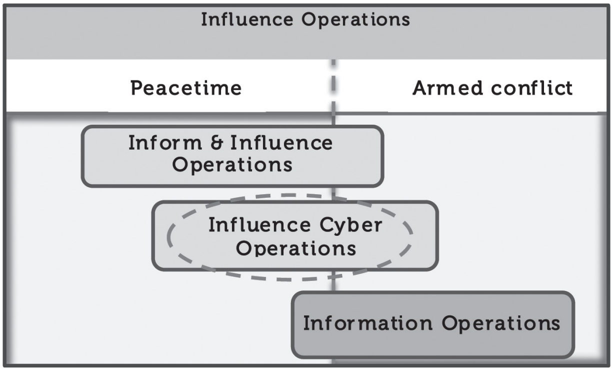
[15] Isaac R. Porche III et.al, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Santa Monica 2013, Page xx.

layer of cyberspace and are designed to influence the behaviour of a target audience.[16] These actions are intrusive as they gain unauthorised access to networks and systems in order to destroy, change or add information. We use the term Influence Cyber Operations (ICOs) for these operations, which we define as follows:

> 'Operations which affect the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences.'

ICOs are therefore activities undertaken in and through cyberspace and qualify as cyberattacks. For the purposes of this article, a cyberattack is understood to be '[a]n act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.'[17] By 'harm', in addition to physical damage, we also comprise the effects on information systems, hence 'direct or indirect harm to a communication and information system, such as compromising the confidentiality, integrity, or availability of the system and any information exchanged or stored.'[18]

FIGURE 1: INFLUENCE OPERATIONS SPECTRUM



3. POLICY FRAMEWORKS FOR INFLUENCE CYBER OPERATIONS

With the advent of the digital domain and the renewed interest in hybrid threats as a result of the Russian aggression against Ukraine in 2014 and its intervention in Syria in 2015, Influence Operations have received greater attention.[19] Influence Operations are an integral part of

[16] We define the logical layer based on the definition of the syntactic layer provided by Martin Libicki as 'the various instructions and services that tell information systems what to do with information. [It] may be said to include operating systems (Oss) and applications. Network syntax clearly includes routing, but also access controls and security, directories, utility servers, and commonly used databases.' in Martin Libicki, *Supra*, p.25.

[17] *NATO Report on Cyber Defence Taxonomy and Definitions*, Enclosure 1 to 6200/TSC FCX 0010/TT-10589/Ser: NU 0289.

[18] *Ibid*.

[19] Jan Joel Andersson and Thierry Tardy, 'Hybrid, what's in a name?', European Union Institute for Security Studies Brief 32, October 2015, http://www.iss.europa.eu/uploads/media/Brief_32_Hybrid_warfare.pdf; Sam Jones, 'Russia steps up Syria Cyber Assault', *Financial Times*, 19 February 2016, http://www.ft.com/intl/cms/s/0/1e97a43e-d726-11e5-829b-8564e7528e54.html#axzz41f9B2xIw.

hybrid warfare, which is the coordinated, overt, and covert use of a broad range of instruments, military and civilian, conventional and unconventional, in an ambiguous attack on another state.[20] Hybrid warfare provides many opportunities for the use of cyber capabilities as one of the broad range of possible non-kinetic or non-violent options. If the main goal of (political) Influence Operations outside of an armed conflict is to destabilise and confuse adversaries, then it could be effective to attack the opponent's digital infrastructure to undermine trust by compromising, altering, disrupting the digital services of both government and private sector through the use of malware.[21]

The strategic outlooks of nations on Influence Operations differ greatly. Where Russia and China have developed more integrated and holistic views, Western states, in general, tend to adopt a much more compartmentalised approach. Given these profound differences in the approaches of Russia and most NATO-members, we will analyse the contradicting strategies and ways in which Influence Operations are conducted.

A. The Russian approach

Russia, more than any other actor, seems to have devised a way to integrate cyber operations into a strategy capable of achieving political objectives.[22] Russia's approach in its power struggle with NATO and the West is based on the acknowledgement that it cannot match the military power of NATO.[23] Strategic advantages must therefore be achieved without provoking an armed response from the Alliance. This is a core element of Russian security policy which is based on the assumption that conflicts between developed nations must remain below the threshold of an armed conflict, or at least below the threshold where it is actually proclaimed to be an armed conflict. This strategy is exemplified by the Gerasimov doctrine (Russian non-linear war[24]) which posits that '[t]he role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of weapons in their effectiveness'.[25] Hence, a greater reliance on the information domain is obvious.

In the Russian view, Information Warfare is conducted in *peacetime*, in the *prelude to war* and in *wartime* in a coherent manner.[26] Information warfare uses:

[20] NATO is also addressing this challenge so that it is 'able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design.', NATO Wales Summit Declaration, 5 September 2014.

[21] Roland Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, FOI-R-2970-SE, p. 20.

[22] James J. Wirtz, 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy' in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* p. 21.

[23] Keir Giles, *Russia's New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, March 2016, p. 26.

[24] Peter Pomerantsev, 'How Putin is reinventing warfare', *Foreign Policy*, 5 May 2014, http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/.

[25] See Mark Galeotti' blog, *In Moscow Shadows*, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[26] A.N. Limno, M.F. Krysanov, 'Information Warfare and Camouflage, Concealment and Deception', *Military Thought*, 2003, vol. 12, no. 2. 'Russian […] writing on the subject has more explicitly retained the more holistic and integrated view of information warfare'. Keir Giles and William Haggestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English', in Karlis Podins, Jan Stinissen, Markus Maybaum (Eds.), *5th International Conference on Cyber Conflict Proceedings*, 2013, NATO CCDCOE Publications, Tallinn, p. 422.

> 'all the means and methods of impacting information, information-psychological, and information-technological objects and information resources to achieve the objectives of the attacking side'.[27]

These include intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems, and propaganda. In this context, be it distributed denial of service attacks (DDoS), advanced exploitation techniques, or RT television, all contribute to the same goals.[28]

From this perspective, using intrusive ICOs as part of a broader Influence Operations strategy makes perfect sense. Given the limited possibilities for attribution and the absence of any real chance of provoking an armed (or even any kind of) response, ICOs are low-risk, low-cost capabilities that can contribute to the destabilisation of an adversary. If the main goal of an Influence Operations campaign is to sow doubt and confusion in order to undermine trust and confidence in the governments of targeted nations, ICOs can certainly contribute to that. The problematic attribution of cyberattacks ensures that it will generally remain unclear who is actually behind the attack, whilst still allowing for a certain degree of plausible deniability when the source of an attack has been determined. One of the major Influence Operations campaigns we have witnessed during the past few years was the involvement of Russia in the Ukraine crisis. However, it is difficult to determine with certainty if these operations did effectively reach their target audience and were able to achieve their intended effects. What is clear, however, is that both IIOs and ICOs have been used as part of a more or less integrated Influence Operation campaign.

B. The Western approach

In democratic societies, there is almost a firewall between the soft power of IIOs and the hard power of covert or clandestine ICOs. This is not only visible in peacetime, but also during military conflicts. There is, of course, a good reason for this as military Information Operations 'often involve deception and disinformation that is effective in war but counterproductive in peace'.[29] As described above, this is a distinction that more authoritarian states do not seem to care about as much.

A major drawback of this compartmentalised approach is that it is proving to be very difficult to develop an integrated, national, approach to Influence Operations. In most Western nations and NATO members, strategic thinking about Influence Operations and Information Warfare was principally done by the military, especially after the disintegration of the USSR. Strategic communications have therefore been mostly led by the defence establishment, but in recent years the need for a more comprehensive approach to Influence Operations has begun to be acknowledged at the highest levels of government.[30]

The distinction between soft power and hard power instruments is key to understanding the limitations of the Western approach. As a matter of fact, the core of IIOs for democracies is to

[27] Timothy Thomas, Supra, p. 142.

[28] David J. Smith. 'How Russia Harnesses Cyberwarfare', *Defense Dossier*, Issue 4, 2012, pp. 7-8.

[29] Joseph Nye, Public Diplomacy and Soft Power, *The Annals of the American Academy of Political and Social Science* 2008; 616; 94, p. 106.

[30] See Paul Cornish, *Strategic Communications and National Strategy*, Chatham House, 2011, p. 4.

tell the truth and act in a manner consistent with its principles. A long term approach built around a carefully developed narrative can only be effective if the facts and messages supporting this narrative are reliable and consistent. Another weakness of this approach is that it assumes a critical thinking and reading ability and interest among the audiences so that the 'most truthful narrative can win' whereas openness to a discourse is a question of faith. The soft power efforts are, by their nature, not only directed at adversary audiences, but also at national audiences and media. This does not mean that Western governments are always truthful in practice, but in theory and as laid down in their policies and strategy documents, this is generally a clearly stated objective.[31]

This compartmentalised approach leaves little room for more clandestine and covert actions, as these will undermine the overall narrative directed at adversary, own and neutral audiences to avoid the risk of undermining one's credibility and narrative. Furthermore, there is a healthy scepticism among populations in democracies that propaganda is not only targeting adversaries but also themselves.[32] Intrusive cyber operations might therefore in the long term do more harm than good by damaging trust among a nation's own population. For democracies, executing coercive Influence Operations, generally, just does not seem to be an option.

In addition, engaging in ICOs that might prove to be intrusive for a state means that it carries out activities that are, in most cases, illegal.[33] Western democracies adhere to the notion that the executive branch of government is bound by domestic laws. This is the fundamental principle of limited government in the legal doctrines of rule of law prevalent in both the common and civil law traditions, and is a vital component of the separation of powers in a democratic regime. This means that the executive can only perform an action if allowed to do so by law. Namely, intelligence services can conduct such operations when, for instance, national security issues are at stake.[34] In that sense, the use of ICOs is rather curbed.

As we have seen, Russia has adopted an integrated approach, which includes ICOs as a tool that can be used in peacetime as well as during an armed conflict. For Western nations, there are solid reasons of transparency, objectivity, and legality to exercise restraint in applying these techniques in a peacetime setting. As a consequence, they have limited the use of ICOs to military operations (MILDEC, CNOs) or specific authorities (primarily intelligence agencies) for very specific purposes.

4. A CLOSER LOOK AT INFLUENCE CYBER OPERATIONS

In this section, we analyse a number of cyber operations whose objective was (or seems to have been) to influence the behaviour of target audiences. It also aims to show how broad the

[31] 'Maintaining transparency and credibility is paramount in the inform line of effort'. See the US Army Field Manual 3-13 on Inform and Influence Activities, January 2013, p. 2-1.

[32] A. R. Pratkanis, 'Winning hearts and minds A social influence analysis', in John Arquilla and Douglas A. Borer (Eds.) *Information Strategy and Warfare A guide to theory and practice*, (New York 2007), p. 78.

[33] See the Convention on cybercrime signed on 23 November 2001 and ratified by 48 nations and the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[34] Operation Cupcake conducted by MI6 in 2011 in Duncan Gardham, 'MI6 attacks al-Qaeda in 'Operation Cupcake'', *The Telegraph*, 2 June 2011, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/MI6-attacks-al-Qaeda-in-Operation-Cupcake.html.

spectrum of ICOs can be as these techniques are all quite common and might be considered low tech as they can be automated, fairly easily outsourced and by the fact that ready-to-use tools are available online. These different activities do, however, qualify as cyberattacks as defined earlier.

Given their effects, ICOs do not reach the level of an armed attack in the legal sense; that is to say that these activities may not prompt an action in self-defence by the injured state pursuant to article 51 of the United Nations Charter. However, given their low intensity, these attacks do not imply that there is a legal void. In this section, some legal comments are provided concerning the different types of techniques we are looking at in order to come up with potential frameworks. Despite these efforts, we will see that these activities are difficult to grasp through the legal lens.

A. Unauthorised access to an information system

Hacking, or gaining access to a computer system, can enable the attacker to modify data for a particular purpose. Hacking critical information infrastructure can seriously undermine trust in national authorities. For example, in May 2014, the group known as Cyber-Berkut compromised the computers of the Central Election Committee in Ukraine.[35] This attack disabled certain functionalities of the software that was supposed to display real time vote-counting. This hack did not hinder the election process, let alone determine its outcome, as voters had to cast an actual physical ballot. It did, however, damage the credibility of the Ukrainian government in overseeing a fair election process. The impact of this type of attack would obviously have been much greater if it had actually influenced the functioning of the voting system. The attack was carried out by a proxy actor and not directly by the Russian government. Although Cyber-Berkut clearly supports Russian policy towards Ukraine, there is yet no definitive proof that these hacktivists have a direct relationship with Russian authorities.[36] This makes denial of involvement by the Russian government not only plausible, but also irrefutable. From the international law standpoint, the use of proxies to conduct such operations makes it almost impossible to relate these activities to a state actor.

Another example is the security breach that affected the US Office of Personnel Management in 2015. Although this was most likely part of an espionage scheme, it was a major embarrassment for the US government and gave the impression that US authorities were not able to protect sensitive information. As Michael Hayden said, this episode is 'a tremendously big deal, and my deepest emotion is embarrassment'.[37]

B. False flag cyberattacks

In April 2015 the French television network TV5 Monde was the victim of a cyberattack from hackers claiming to have ties with Islamic State's (IS) 'Cyber Caliphate'.[38] TV5 Monde said its TV-station, website, and social media accounts were all hit. In addition, the hackers

[35] Nikolay Koval, 'Revolution Hacking', in Kenneth Geers (Ed.), *Cyber War in perspective: Russian Aggression against Ukraine*, NATO CCDCOE Publications, Tallinn, 2015.

[36] Tim Maurer, 'Cyber Proxies and the Crises in Ukraine', in Kenneth Geers (Ed.), *Cyber War in perspective: Russian Aggression against Ukraine*, NATO CCDCOE Publications, Tallinn, 2015, p. 85.

[37] 'Michael Hayden Says U.S. Is Easy Prey for Hackers', *Wall Street Journal*, 21 June 2015, http://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058.

[38] Pierre Haski, 'Des cyberdjihadistes attaquent TV5 Monde : « Puissance inouïe »', Rue89, 9 April 2015, http://rue89.nouvelobs.com/2015/04/09/lattaque-tv5-cyber-djihadiste-dune-ampleur-sans-precedent-258584.

posted documents purporting to be ID cards of relatives of French soldiers involved in anti-IS operations. TV5 Monde regained control over most of its sites after about two hours. In the aftermath of the January 2015 terrorist attacks on Charlie Hebdo, it was quite obvious to the general public and to the investigators that the attackers had ties with the IS organisation.

In June 2015 security experts from FireEye involved in the investigation of the hack revealed that Russian hackers used the pseudonym of IS 'Cyber Caliphate' for this attack. According to them, the Russian hacker group known as APT28 (also known as Pawn Storm, Tsar Team, Fancy Bear and Sednit) may have used the name of IS as a diversionary strategy. The experts noticed a number of similarities in the techniques, tactics, and procedures used in the attack against TV5 Monde and by the Russian group.'[39] This can therefore be qualified as a false flag cyberattack where the use of specific techniques (IP spoofing, fake lines of code in a specific language), will result in misattribution.[40]

Why Russia would hack, or sponsor and condone someone else hacking, a French TV station, and pin the blame on an extremist organisation is unclear, since there seems to be no direct correlation with Russian policies. The only discernible rationale behind these attacks, if conducted by Russia, is to sow confusion and undermine trust in French institutions in a period of national anxiety. TV5 Monde can be blamed for not properly protecting its networks and looking like foolish amateurs, and the French government was seemingly unable to respond in an effective way. Although there is no direct connection, it could be argued that any action that undermined the French government may have led it to act in ways favourable to Russian interests.

Here again, plausible deniability provides enough cover not to worry about the legality of such actions or any response of the victim. The fact that only months later it was discovered that there might be a link to the Russian government highlights the very limited risk of repercussions or countermeasures.

C. DDoS attacks

The most common ICOs are distributed denial of service (DDoS) attacks and these provide a clear illustration of the disruptive effects of ICOs in general. The most famous DDoS attacks were the coordinated ones that occurred in April 2007 in Estonia, during the civil unrest resulting from the government's decision to move a Soviet memorial statue.[41]

DDoS attacks are probably still the prevailing option for many actors, as gaining access to

[39] According to FireEye '[t]here are a number of data points here in common […] The 'Cyber Caliphate website', where they posted the data on the TV5 Monde hack was hosted on an IP block which is the same IP block as other known APT28 infrastructure, and used the same server and registrar that APT28 used in the past.' See Pierlugi Paganini, 'FireEye claims Russian APT28 hacked France's TV5Monde Channel', *Security Affairs*, 10 June 2015, http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html.

[40] We define a false flag attack as 'a diversionary or propaganda tactic of deceiving an adversary into thinking that an operation was carried out by another party'. See Mauno Pihelgas (ed.) *Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks*, https://ccdcoe.org/sites/default/files/multimedia/pdf/False-flag%20and%20no-flag%20-%2020052015.pdf.

[41] See Andreas Schmidt, 'The Estonian Cyberattacks', in Jason Healey (Ed.) *A Fierce Domain: Conflict in Cyberspace*, 1986-2012, 2013, published by the Atlantic Council.

a botnet is fairly easy and affordable.[42] DDoS attacks are used to overwhelm the target's resources (degradation) or stop its services (disruption). Attacks only affect the availability of internet services and do not infringe on the confidentiality or integrity of networks and data. The objective of these attacks is, therefore, typically to undermine the targets' credibility.

Although technical solutions exist to mitigate their effects, they are still widely used to embarrass governments or other organisations.[43] In 2014 and 2015, NATO websites were the victims of such a campaign and the disruption prompted significant concern, as the main aim of these attacks was to embarrass and disseminate anti-NATO propaganda and to undermine NATO's readiness to defend itself in cyberspace.[44] They also have a 'paintball effect' as they may give the impression of a severe cyberattack.[45] Last but not least, it is very unlikely that a DDoS attack may be considered as a violation of international law, thus creating grounds for a state to lawfully conduct countermeasures against another state.[46]

D. Website defacements

Although most website defacements or hacks of Twitter accounts have only very limited impact, their results can be quite catastrophic. In 2013 the Twitter account of the Associated Press was hacked and a message claiming the White House was under attack was posted. This sent the stock markets down 1 percent in a matter of seconds. With High Frequency Trading, short interruptions as a result of false messages can have profound financial repercussions.[47]

However, in most cases, website defacements are comparable to graffiti and can be classified as vandalism. Technically, they are not very complicated and, again, the effect lies mainly in the embarrassment it causes to the target. The aim is to sow confusion and undermine trust in institutions by spreading disinformation or embarrass the administrators for poor network defence. The effectiveness of the attack therefore lies in the media reaction;[48] the exposure is far more important than the technical stunt itself. These attacks are minor stings, but taken together they have the potential to erode credibility. Their long term effectiveness, however, is questionable, as people become aware of their limited impact and network security is improved.

[42] One of the most used techniques and their number is rising every year. https://www.stateoftheinternet.com/security-cybersecurity-attack-trends-and-statistics.html. 'Attackers can rent DDoS attack services for as little as $5, letting them conduct a few minutes-worth of DDoS attacks against any chosen target' in *The continued rise of DDoS attacks*, Symantec Whitepaper, 21 October 2014, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf.

[43] 'DDoS on the Move: in Q1 More Countries Suffered Botnet Attacks, Kaspersky Lab Stats Show', 29 May 2015, http://www.kaspersky.com/about/news/virus/2015/DDoS-on-the-Move-in-Q1-More-Countries-Suffered-Botnet-Attacks-Kaspersky-Lab-Stats-Show.

[44] Jeffrey Carr, 'Cyber-Berkut and Anonymous Ukraine: Co-opted Hacktivists and Accidental Comedians', *Digital Dao*, 15 March 2014, http://jeffreycarr.blogspot.ro/2014/03/cyber-berkut-and-anonymous-ukraine-co.html.

[45] Thomas Rid and Peter Mc Burney state that 'low-potential cyber weapons resemble paintball guns: they may be mistaken for real weapons, are easily and commercially available, used by many to play and getting hit is highly visible', in Thomas Rid and Peter McBurney, 'Cyber Weapons', *RUSI Journal*, 157:1, 6-13, DOI, http://www.tandfonline.com/doi/abs/10.1080/03071847.2012.664354#.Vrm6V7J95aQ.

[46] For legal analysis of the 2007 Cyberattacks on Estonia see Kadri Kaska et al., *International Cyber Incidents; Legal Considerations*, NATO CCDCOE Publications, 2010; Michael Schmitt, 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law, *Virginia Journal of International Law*, Vol. 54:3, 2014.

[47] Heidi Moore and Dan Roberts, 'AP Twitter hack causes panic on Wall Street and sends Dow plunging', *The Guardian*, 23 April 2013, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

[48] Brian Fung and Andrea Peterson, 'The Centcom hack that wasn't', *The Washington Post*, 12 January 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/.

E. Doxing

Another technique that has been widely used in recent years is 'doxing' (or 'doxxing'), which is the practice of revealing and publicising information on an organisation (e.g. Sony Corporation[49]) or an individual (e.g. John Brennan[50]) that is private or classified, so as to publically shame or embarrass targets. There are various ways to obtain this information, ranging from open sources to hacking. This type of action is on the rise and if the data of people like the director of the CIA is accessible, that means that everyone's might be.[51]

Doxing may be used for political purposes. For example, in February 2014, Victoria Nuland, then US Assistant Secretary of State for European and Eurasian Affairs, made a rather obscene comment about the European Union in a telephone conversation with the US Ambassador to Ukraine.[52] This type of incident is embarrassing, but more importantly, can create divisions among allies and jeopardise a common policy to address a crisis situation.

Doxing can be an offshoot of an espionage operation, and thus turned into an ICO. Information obtained through a cyberattack as part of an espionage operation can then be disclosed to undermine the adversary. These activities cannot be qualified as a use of force, or be deemed of a coercive nature under international law.[53]

F. Limited response options

After this short overview, one can see the difficulty in grasping the full implications of these ICOs that span a wide spectrum of activities; from the technically savvy to those that are more content-oriented. The common traits are that they have generally limited impact on the attacked party and their success lies in the response or lack thereof. As a matter of fact, it is difficult to counter an ICO as the course of action to respond to them might actually result in a counterproductive outcome or be disproportionate, and thus lead to escalation.

The international law of state responsibility provides grounds to determine if a state has breached an obligation under customary international law (e.g., violation of sovereignty, violation of the principle of non-intervention) in a way that would be deemed an internationally wrongful act.[54] To identify such a violation, it is necessary to determine whether the actor behind a cyber operation can be linked to a state. In order to achieve that, it is necessary to determine whether that state exercises 'effective control' over the group or organisation in question. According to

[49] Kim Zetter, 'Sony got hacked, hard, what we know and don't know so far', *Wired Magazine* 3 December 2014. http://www.wired.com/2014/12/sony-hack-what-we-know/.

[50] Sam Thielman, 'High school students hack into CIA director's AOL account', *The Guardian*, 19 October 2015. http://www.theguardian.com/technology/2015/oct/19/cia-director-john-brennan-email-hack-high-school-students.

[51] Bruce Schneier, 'The rise of political doxing', *Motherboard*, 28 October 2015, http://motherboard.vice.com/read/the-rise-of-political-doxing.

[52] Anne Gearan, 'In recording of U.S. diplomat, blunt talk on Ukraine', *The Washington Post*, 6 February 2014, https://www.washingtonpost.com/world/national-security/in-purported-recording-of-us-diplomat-blunt-talk-on-ukraine/2014/02/06/518240a4-8f4b-11e3-84e1-27626c5ef5fb_story.html.

[53] See Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage', in Anna-Maria Osula and Henry Rõigas (Eds), *International Cyber Norms, Legal, Policy & Industry Perspectives*, NATO CCDCOE Publications, 2016.

[54] See James Crawford, *International Law Commission's Articles on State Responsibility, Introduction, Text and Commentaries*, Cambridge University Press, 2002, The forthcoming Tallinn Manual 2.0 will specifically address the issues of State Responsibility pertaining to cyberspace.

the stringent criteria defined by the International Court of Justice, it is difficult to relate many actions in cyberspace to a state, making the options to respond highly limited.[55]

5. CONCLUSIONS AND RECOMMENDATIONS

The attraction of ICOs for states lies mainly in the fact that they are difficult to attribute, and thus provide a high degree of plausible deniability and limited risk of provoking a strong or quick response from the target nation. However, as we have seen, their scope and applicability are restricted as their impact will generally be limited to harassing and annoying a target audience. In most cases, they are not suited to achieving a profound shift in attitude of a target audience or policy of a nation. Although Russia has embarked on a long term and coordinated IIO campaign against NATO and western democracies, its impact on public opinion is limited and its effectiveness will likely decrease as populations become more aware of Russian intentions and the actual impact of the campaign.[56] This is especially relevant in regard to the ICOs orchestrated by Russia. The more target audiences and organisations become aware of the need for adequate protection of their digital infrastructure and the limited long term impact of cyberattacks, the less useful they will become. Most attacks that can be labelled as ICOs are not highly complex and make use of ‘low hanging fruit’; the exploitation of those networks with the weakest defences.

ICOs will, however, remain a nuisance and be able to create a certain amount of confusion. As part of a broader IO campaign, they can fuel an already existing sense of insecurity, and thereby support the overall narrative of the campaign. A study conducted by the Chapman University showed, for instance, that Americans fear a cyber terrorist attack more than a physical terrorist attack.[57] This shows that an adversary can exploit the fear of the unknown, whether that fear is realistic or mostly imaginary.

For NATO members and other democracies, the use of ICOs outside of an armed conflict situation will be limited. As these operations involve intrusive measures, the legal grounds for launching these kinds of attacks are generally lacking. In principle, only the intelligence agencies possess the legal mandate to enter networks in foreign countries, and then only under very specific and supervised conditions.[58] In addition, the importance of transparency of government actions in democracies limits the options for employing covert operations to influence the opinions and attitudes of target audiences as such operations are often associated with PSYOPS or propaganda and thus are frowned upon by public opinion and the media.

[55] Michael Schmitt and Liis Vihul, ‘Proxy Wars in Cyberspace: The Evolving International Law of Attribution’, *Fletcher Security Review*, Vol I, Issue II Spring 2014.

[56] ‘It has been argued that information campaigns and cyber tools at the disposal of Russia have had a significant influence on the crisis in Ukraine. So far no one has convincingly shown the real tangible effects of Russian Information warfare, its army of internet trolls and the use of other cyber-attacks’. See Jyri Raitasalo, ‘Hybrid Warfare: where’s the beef?’ *War on the Rocks*, 23 April 2015, http://warontherocks.com/2015/04/hybrid-warfare-wheres-the-beef/.

[57] See the Chapman University Survey on American Fears in 2015, http://www.chapman.edu/wilkinson/research-centers/babbie-center/survey-american-fears.aspx.

[58] See for example the FISA (Foreign Intelligence Surveillance Act) in the United States, which provides for strict limitations on foreign surveillance.

To raise awareness, it is also necessary to increase transparency.[59] The media need to be provided with reliable and verifiable information so that the general audience is better informed, and to minimise exaggeration regarding the effects of certain cyberattacks. Additionally, and deriving from this transparency issue, states and corporations will have to learn to deal better in a more transparent and less convulsive way with leaks that are bound to happen, as a secretive and evasive response will merely increase their impact.[60]

In response to ICOs, it is therefore essential that government officials and the public at large have a fundamental grasp of the nature and impact of the multiple kinds of cyberattacks that are possible. They must be aware that hacking the webserver of a TV station does not constitute a serious threat to the security or governability of a nation. Hence, apart from the obvious importance of proper defence of networks and systems, the primary instrument for nations to counter ICOs is to raise cyber awareness among the population at large as well as the bureaucratic and political elite. An important step towards this is to tone down the hyperbole in the media, which is too easily tempted to label everything as ‘cyber war’.

[59] ‘Fortunately, the antidote to Netwar poison is active transparency, a function that democracies excel in’. In Robert Brose, ‘Cyber War is not Net War, Net War is not Cyber War’ in *7th International Conference on Cyber Conflict Proceedings*, NATO CCD COE Publications, 2015, p. 48.

[60] Henry Farrell and Martha Finnemore, ‘The end of hypocrisy: American Foreign Policy in the Age of Leaks’, *Foreign Affairs*, 15 October 2013.