Cybersecurity: A National Security Issue?

https://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/

DANIELE HADI IRANDOOST, MAY 3 2018

It is not unusual to hear that despite its many benefits cyberspace has, at the same time, opened doors for those intent on achieving criminal aims. Cyber blackmail, identity theft and fraud are some of the ways in which these have been previously witnessed. As historical cases demonstrate, however, threats from cyberspace do not merely end there. In fact, they can be so expansive they could harm entire nations (Clarke & Knake, 2010). After all, the recent *Worldwide Threat Assessment of the US Intelligence Community* (2016) put 'Cyber and Technology' as the top priority ahead of other prominent threats including terrorism, the proliferation of weapons of mass destruction and counterintelligence. Compared to a decade ago – and before – when cyber and technology were at the bottom of this list, this is an alarming development that begs significant attention. Given this circumstance, it should not be surprising that the US established the new Cyber Command in 2009 to ensure cybersecurity, or indeed when it provided the Defense Department with 6.7 billion dollars in 2017 for cyber operations (Lyngaas, 2016).

Bearing in mind that such things require a significant amount of taxpayers' money, a clear justification is in order. Above all, are we facing an existential threat to our way of life from attacks that originate in cyberspace? More specifically, should we consider cybersecurity a matter of national security and to what extent? This essay intends to address this question in four parts. Whilst the first part sets out an overview of why cybersecurity may be considered an *absolute* matter of national security, the second examines why the opposite might be the case. The first two sections thus set the stage for a balanced discussion in the third section, in which the methodology of the first two are criticised and an alternative is proposed and examined; it is specifically maintained that cyber threats are 'potentially' destructive to national security. The final section, lastly, argues that the way in which cybersecurity is faced and perceived by nations varies from one to another according to differences in context, principally in the sense of technological development. Ultimately, the relevance of this essay for policymaking lies in clarifying the extent to which different actors – governments, international institutions, private individuals, or a combination of these – should be responsible for cybersecurity. Before moving on, it must be noted that threats to national security are defined in this essay as existential in nature impacting a nation on a strategic or political level (Buzan, et al., 1998: 21ff).

Richard A. Clarke, John Arquilla, David Ronfeldt and Peter L. Levin amongst others all believe that cyberwar is inevitable and will sooner or later lead to a catastrophe in which an entire nation (the USA especially) is brought down to its knees while a great many of its people are killed in the process – perhaps in the form of a 'cyber-Pearl Harbor' or 'cyber-9/11' (Clark & Levin, 2009; Arquilla & Ronfeldt, 1993; Miller & Shanker, 2012). Clarke and Knake's famous scenario offers a particularly representative description of such an incident. In brief, this scenario describes a series of synchronised attacks undertaken in a manner unlike any before, whereupon various arms of Critical National Infrastructure (CNI) including the power grid, communication networks, as well as the financial and transportation systems amongst others are all attacked and crippled at the same time (Clarke & Knake, 2010: 167ff.). In this instance, Clarke and Knake add, the government has virtually lost control of the nation, military and civilian structures, and is potentially left vulnerable to a conventional kinetic attack (that is, by an enemy whose leadership has decided to occupy territory and subdue the population).

Fundamentally, this sentiment is justified in terms of several (supposed) characteristics unique to cyberspace. The most important of these concerns the superiority of offence over defence in cyber operations; an outlook that may partly be attributed to cyberspace's original design, which evolved initially from the US Department of Defense's ARPANET network. As it happens, cyberspace was conceived in the first place as a highly complex and

interconnected medium intended for open and unlimited communication between a variety of users. Since, however, no one at the time could foresee dangerous possibilities in the future, defence and security were unsuspectingly ignored. It stands to reason, on that premise, regardless of the many security measures that are always taken against cyber threats, inevitable architectural flaws within the system give rise to vulnerabilities that will perpetually remain exploitable (Arquilla, 2012). What makes the matter worse is that as digital networks and actors capable of undertaking cyberattacks grow rapidly, the odds of having such vulnerabilities exploited multiply by the day. This is not only because of the general surge in *points of attack* (targets) thanks to an expanding digital interconnectedness (in depth, reach and 'surface area'), but also due to a rise in the *number* of cyberattacks as more actors increasingly gain the capability and knowhow to operate in cyberspace. In connection therewith, it is not unexpected that Clarke and Knake (2010: 147ff.) recognise the US as the most vulnerable nation in the world – assuming that it may also be the most interconnected.

Be that as it may, another important feature of cyberspace that is said to contribute to the superior position of offence over defence is in regard to the 'problem of attribution', anonymity, or plausible deniability (even a 'Russian-style' denial) (Goldsmith, 2013: 131ff.). In short, these refer to the difficulty in confirming an attacker's identity within cyberspace; a predicament that not only hinders victims from undertaking retaliation, but one that diminishes potential enemies' fear of reprisal by the victims, undermining thereby what effectiveness deterrence could have had as an instrument of cybersecurity (alongside 'cyber defence') (Robinson, et al., 2015). To a large extent, this is because – unlike the days of the Cold War when only a handful of states possessed nuclear weapons – cyberattacks today may readily be carried out from both within and outside a state by a variety of state and non-state actors. At the same time, however, what makes the matter worse is the difficulty (if not the impossibility) of tracing an attack to its origin or identifying the intentions of a perpetrator behind a computer; it could be highly possible, for instance, for accidents to occur due to collateral damage or a misunderstanding (Goldsmith, 2013: 130). Furthermore, the fact that international norms and laws on cyberwar still require significant progress and development does not help 'cyber deterrence' (and therefore cybersecurity) either (Walker, 2015).

With those in mind, it is now time to consider what others have proposed in direct contrast. Thomas Rid, above all, argues cyberwar will never take place in the future (other authors who hold very similar views include Jon R. Lindsay, 2013; Brandon Valerian & Ryan C. Maness, 2014). According to Rid, this is because war in cyberspace (cyberwar) does not meet the three criteria essential for defining war in its traditional, Clausewitzian sense: war as potentially violent, instrumental (that is, as a means to an end), and political in nature (Rid, 2012: 7f.). In this respect, he adds that no single cyber 'incident' of any kind in history has ever met all three altogether, and even those which may be said to have come close to completing at least one criterion are rare and questionable (Rid, 2012: 10ff.). More than that, he especially posits that no cyber 'incident' has ever taken a single life, and never will because of the many obstacles that prevent the possibility of a kinetic effect.

Rid believes the chief obstacle in this regard is that it is rather defence that is advantageous over offence, not the other way around. He believes sophisticated attacks – which are assumed to be far more intense and, therefore, highly damaging – will never pose a threat to cybersecurity due to the sheer difficulty in their execution (Rid, 2013: 80ff.). As an illustration, he points to the Stuxnet attack on the Iranian uranium enrichment facility in Natanz around 2009-10. He argues not only was there a need for an 'agent' on the ground to skip the 'air-gapped' network (by means of a USB thumb drive), but also the need for long-term planning and management on the part of the US and – allegedly – Israel, along with a high level of expertise, technical knowledge, and significant expenditures (Rid, 2012: 17ff.). By and large, Rid argues these difficulties resulted in an ineffective operation that only had a temporary and limited effect on Iran's ability to create nuclear weapons (Rid, 2013: 85f.). Rid additionally notes that fear of self-inflicting collateral damage further discourages states from engaging in offensive attacks – suggesting yet again that offence is somewhat inferior to defence (Rid, 2013: 85).

From this consideration and others,[1] what may be inferred thus far is that there is no clear consensus about the extent to which there is a real possibility for cyberwar. It appears, rather, that various theoretical discussions largely continue without end; they have, for all intents and purposes, become polarised. Notwithstanding, it must be stated that there is an alternative view, one that is critically balanced and offers nuanced insight into the ways in which cyber threats may undermine national security. This view is largely applied – at least implicitly, in terms of a theoretical

approach – in the two recent works of Kristan Stoddart (2016a; 2016b) and, perhaps in some ways, that of Eric Byres & Justin Lowe (2004). This view is specifically based on a technical understanding of various aspects behind cybersecurity (drawn in particular from hard, empirical evidence) and a critical insight gained from the humanities (which, amongst other things, study social constructs). It is the interdisciplinary combination between the broader computer sciences and the humanities that is timely and of necessity now, considering the stalemate that has persisted so far in consequence of prevailing discussions that have polarised 'cyber studies'.

Therefore, when cybersecurity is examined from several angles on the technical aspects, we find trends and evidence indicate that ultimately there lies a great 'potential' for damage from cyberattacks. Specifying the more important aspects can provide a useful starting-point to substantiate this proposition. To begin with, one angle concerns *actors* that are capable of exploiting cyberspace for different purposes. As alluded to earlier, today these could include states, hacktivist groups, individual criminals, terrorists, syndicate organisations and even privateers – all of which can be transnational in nature. One may, then, consider another angle regarding the *modus operandi* of cyberattacks: such as 'backdoors', 'phishing', 'denial of service attacks', 'clickjacking', 'direct-access attacks' and 'privilege escalation' amongst many others. This may, subsequently, be followed by a consideration of possible *targets*: namely, the government, military, healthcare and financial systems, 'Internet of Things', large corporations, major industries, nuclear and chemical plants, aviation, other critical infrastructure sectors, not to mention consumer devices such as smartphones. In turn, *vulnerabilities* found in systems associated with cyberspace would be worth analysing next: such as, tampered hardware components, software architectural flaws, unprotected communication networks, poor vetting of personnel within high-value facilities, poor organisation and management of security, lack of strict physical policing in high-value industries and buildings areas, as well as social engineering.

Ultimately, what the preceding technicalities point to are the wide-ranging possibilities and opportunities that could potentially lead to a breach of a nation's cybersecurity. In this respect, recent as well as distant examples evidence how such possibilities have already occurred and could equally do so again in other ways in the future. With that said, a few notable examples of cyberattacks in history would be fitting to recount here: including the aforementioned Stuxnet attack (on a major nuclear facility in Iran), the 2007 attack on Estonia (affecting the government, financial system and communication networks amongst others), the 2008 attack on Georgia (affecting command and control and making vulnerable the military against a conventional attack), and the attack on the Japanese multinational conglomerate corporation, Sony (which led to its loss of a significant amount of data and financial resources). When such matters are considered from a technical perspective along with their effects on real life (social aspects, that is), one may observe that there is an increasing trend towards 'potential' cyber incidents of a wide-ranging scale, harming nations at a strategic or political level. The above approach, accordingly, not only guides 'cyber studies' to a more critical understanding of dangers to cybersecurity, it also discredits claims by the likes of Thomas Rid who argue that there is no danger.

Indeed, it is worth mentioning here that even cybercrime which is usually seen as a matter concerning individual civilians, can equally target national infrastructures for, say, personal gain (financial or otherwise) (Bartlett, 2015). One is particularly reminded of transnational criminals sponsored by foreign governments to undertake 'plausibly deniable' cyber operations: an illustrative example being the 2007 cyberattack on Estonia, allegedly undertaken by a group of Russian hackers on behalf of the Russian government.

Notwithstanding the foregoing, it is important to note that not all states will face and perceive cybersecurity in the same way. This is because context – above all – defines the extent to which different kinds of cyber threats undermine national security. This view is drawn specifically from Forrest Hare (2010), whose adaptation of Barry Buzan's framework of analysis offers a useful tool for examining factors that determine what cyber threats different states might face. This framework of analysis is namely based on two factors: 'power' and 'socio-political cohesion' (Hare, 2010: 215). Briefly, while the former refers to cyber capabilities (both offensive and defensive) at a state's disposal, the latter essentially refers to domestic unity from a social and political standpoint. To illustrate how the framework could be applied in practice, an example may be sufficient.

North Korea is usually considered to be one of the least vulnerable nations against cyber threats (Clarke & Knake, 2010: 147ff.). For the most part, this characteristic may be attributed to the nation's lack of adequate infrastructure

connected to cyberspace – which, as an economically backward nation, is certainly not surprising (Clarke & Knake, 2010: 147ff.). What is noteworthy in this regard, however, is that North Korea's limited access to and use of cyberspace essentially limits serious points of attack (vulnerabilities) that potential enemies could target. The obvious implication, then, would be that (excepting, perhaps, its leadership or military industrial programmes) North Korea – as a state – could effectively remain immune from cyber threats. What is more, as the North Korean population does not seem to have access to global networks in the same way people in other nations do, it would be highly unlikely for cyber subversion to find any targets in North Korea. For those reasons, it would not be unfair if one considered cybersecurity an insignificant matter of national security from the North Korean standpoint.

All the same, it should not be forgotten that strengths, or weakness for that matter, are always dynamic; for context is an ever-changing factor. The Snowdon revelations or certainly the release of classified documents by WikiLeaks, which caused a fury of debates on surveillance and rights in the US, illustrate how weaknesses in 'socio-political cohesion' can gradually become more important in time (Hare, 2010: 220f.: DeNardis, 2012: Pieterse, 2012: Giles & Hagestad II, 2013).

With those in mind, it should be mentioned here a nation's general technological development is the fundamental factor that underlies both 'socio-political cohesion' and 'power'.[2] Developing states such as Haiti, Bhutan and Cambodia amongst others do not depend on ICT in the same way as do developed states. What this suggests, therefore, is that cybersecurity may only be considered a national security issue when a state is *sufficiently* developed to rely to some extent on cyberspace.[3]

All in all, theoretical discussions on cybersecurity for policymaking purposes have their limitations and have currently reached a plateau as demonstrated in the first two sections of this essay – on why cyberwar is or is not inevitable. The subsequent section, then, proposed the application of a more balanced approach, based on hard evidence and technical knowledge allied with critical insight from the humanities. Lastly, thereafter, the final section advanced how different states face different cyber threats and may therefore perceive cybersecurity differently to others. On the whole, a question that needs to be considered now, particularly in liberal-democracies, is on the allocation of specific responsibilities to public and private actors to ensure cybersecurity without, at the same time, compromising civil liberties. Even though scholarly steps have already been taken in this regard, they are merely infrequent. Again, Kristan Stoddart's (2016b) most recent article on the UK's governance of cybersecurity and the need for balanced cooperation and information-sharing between the government and the private sector is one of few examples. To conclude, it is fair to say from the discussion hitherto that a combined understanding of the technical aspects of cybersecurity along with insight from the humanities is currently of utmost significance to national security, particularly for those states that are sufficiently developed. The numerous cyber incidents that have taken place in the past provide a sound demonstration to this argument. Cybersecurity is, thus, a crucial national security issue that needs to be understood carefully and thoroughly.

Bibliography

Arquilla, J., 2012. *Cyberwar is Already Upon Us: But Can it be Controlled?.* [Online]
Available at: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/
[Accessed 30 April 2017].

Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is Coming!. *Comparative Strategy,* 12(1), pp. 141-165.

Bartlett, J., 2015. *The Dark Net: Inside the Digital Underworld.* London: Windmill Books.

Betz, D., 2012. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies,* 35(5), pp. 689-711.

Betz, D. J. & Stevens, T., 2011. *Cyberspace and the State: Towards a Strategy for Cyber-Power.* Abingdon: Routledge/International Institute for Strategic Studies.

Buzan, B., Wæver, O. & Wilde, J. d., 1998. *Security: A New Framework for Analysis.* Boulder, Colo.: Lynne Rienner.

Byres, E. & Lowe, J., 2004. *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems.* Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies.

Carlin, J., 1997. *A Farewell to Arms.* [Online]
Available at: http://archive.wired.com/wired/archive/5.05/netizen.html
[Accessed 30 April 2017].

Clapper, J. R., 2016. *Worldwide Threat Assessment of the US Intelligence Community: Senate Armed Services Committee.* [Online]
Available at: https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf
[Accessed 30 April 2017].

Clarke, R. A. & Knake, R. K., 2010. *Cyber War: The Next Threat to National Security and What to do About it.* New York: HarperCollins Publishers.

Clark, W. K. & Levin, P. L., 2009. Securing the Information Highway: How to Enhance the United States' Electronic Defenses. *Foreign Affairs,* 88(6), pp. 2-6, 8-10.

DeNardis, L., 2012. Hidden Levers of Internet Control. *Information, Communication and Society,* 15(5), pp. 720-738.

Gartzke, E., 2013. The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth. *International Security,* 38(2), pp. 41-73.

Giles, K. & Hagestad II, W., 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In: K. Podins, J. Stinissen & M. Maybaum, eds. *2013 5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, pp. 413-429.

Goldsmith, J., 2013. How Cyber Changes the Laws of War. *European Journal of International Law,* 24(1), pp. 129-138.

Hare, F., 2010. The Cyber Threat to National Security: Why Can't We Agree?. In: C. Czosseck & K. Podins, eds. *Conference on Cyber Conflict Proceedings.* Tallinn: NATO CCD COE Publications, pp. 211-225.

Junio, T., 2012. How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate*Journal of Strategic Studies,* 36(1), pp. 125-133.

Kello, L., 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security,* 38(2), pp. 7-40.

Libicki, M. C., 2012. Cyberspace Is Not a Warfighting Domain. *Journal of Law and Policy for the Information Society,* 8(2), pp. 325-340.

Liff, A. P., 2012. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* 35(3), pp. 401-428.

Liff, A. P., 2013. The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. *Journal of Strategic Studies,* 36(1), pp. 134-138.

Lindsay, J. R., 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies,* 22(3), pp. 365-404.

Lyngaas, S., 2016. *The Business of Federal Technology.* [Online]

Available at: https://fcw.com/articles/2016/02/09/dod-it-budget-cyber.aspx
[Accessed 30 April 2017].

Miller, E. B. & Shanker, T., 2012. *Panetta Warns of Dire Threat of Cyberattack on U.S.* [Online]
Available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0
[Accessed 30 April 2017].

Pieterse, J. N., 2012. Leaking Superpower: WikiLeaks and the Contradictions of Democracy. *Third World Quarterly,* 33(10), pp. 1909-1924.

Rid, T., 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35(1), pp. 5-32.

Rid, T., 2013. *Cyberwar and Peace: Hacking Can Reduce Real-World Violence.* [Online]
Available at: https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace
[Accessed 30 April 2017].

Robinson, Jones, K. & Janicke, H., 2015. Cyber Warfare: Issues and Challenges. *Computers & Security,* Volume 49, pp. 70-94.

Stoddart, K., 2016a. Live Free or Die Hard: U.S.–UK Cybersecurity Policies. *Political Science Quarterly,* 131(4), pp. 803-842.

Stoddart, K., 2016b. UK Cyber Security and Critical National Infrastructure Protection. *Political Science Quarterly,* 131(4), pp. 803-842.

Valerian, B. & Maness, R. C., 2014. The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11.*Journal of Peace Research,* 51(3), pp. 347-360.

Walker, P. A., 2015. Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace. In: *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace.* Tallinn: NATO CCD COE Publications, pp. 93-104.

Notes

[1] Another debate concerns, for instance, Martin Libicki's (2012) proposition that cyberspace is not a warfighting domain because of its malleability, operational dissimilarity with wars in the physical realm and the multiple media in which actors may operate. To oppose this view, however, Lucas Kello (2013: 22ff.) notes that the Clausewitzian approach utilised by Libicki misses the point as it ignores not only non-state actors, but also the importance of effect (or consequence) which arise out of cyberattacks. Another debate, likewise, is seen in Gartzke's (2013: 47) criticism of the 'problem of attribution'. He argues that the attribution problem can only lead to the 'credibility problem', which is the inability to influence decisions politically as a result of remaining anonymous – denoting, in turn, the superiority of offence over defence.

[2] In Hare's article, technological development as a determining factor is not appropriately acknowledged.

[3] Where this threshold should be drawn, however, is obviously open to question and remains a topic for another essay.

Written by: Daniele Hadi Irandoost
Written at: Aberystwyth University
Written for: Dr. Kristan Stoddart
Date written: May 2017