ARI 16/2020
27 February 2020

# The Future of Values in Cyber Security Strategies

**Danny Steed** | Author, Public Speaker and Consultant | @TheSteed86

## Theme

While national cyber security strategies have proliferated worldwide in the past decade, most have been overwhelmingly focused on resilience at the expense of political values. This paper addresses the challenges that have arisen from an overly technical focus on cyber security that has failed to consider the application of value sets in strategy creation.

## Summary

The efforts and public expenditures that have been committed to the pursuit of cyber security in the past decade are no doubt vast. In numerous nations these efforts have included the creation of several iterations of national cyber security strategy to guide public efforts. Despite such investment of both public monies as well as intellectual and policy capital however, it would be difficult to claim that the state of cyber security is much improved.

Indeed, even subject experts and seasoned professionals within cyber security will be quickly overwhelmed with the available data reported by numerous outlets on the pernicious and ever-growing volume of cybercrime worldwide. In the face of conflicting real-world evidence of a problem that is barely improving, a hard question must be asked: do our national cyber security strategies carry flaws?

This author contests that this is the case, arguing that our present strategies have been overly focused on technological matters and establishing national resilience, to the detriment of values establishment that would aid the development of normative behaviour. With the scale of cyber security challenges faced by nations, and the lack of consensus internationally to temper the geopolitical future of cyberspace, a concerted drive in values assertion is a missing element of cyber security strategies that should be taken seriously.

## Analysis

There are of course dozens of national cyber security strategies to use as examples. For the purposes of this article, those from the UK and the Netherlands will suffice. The UK is currently finishing its third cyber strategy iteration, due to compete in 2021. The strategy declared its aim as a vision in 2021 of a UK 'secure and resilient to cyber threats, prosperous and confident in the digital world.'[1] This is built on with a model of Defend, Deter and Develop. The logic of this triptych is to establish resilience in Defend, Deter

[1] HM Government, United Kingdom (2016), 'National Cyber Security Strategy 2016-2021', p. 9, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

bad actors by becoming a hardened target, and Develop indigenous talent through numerous schemes to plug a digital skills gap. Immediately the critical reader will note that values development and normative standards are not primary concerns represented in this strategy.

Others will contest this perspective, arguing that the strategy's chapter 8 on International Action does indeed address the need for normative development. To take this at face value would be immature however, as UK efforts have remained overwhelmingly focused on technical resilience measures –most notably in the establishment of the UK's National Cyber Security Centre– and by noting the paralysis of international efforts in the UN Government Group of Experts on cyber. The UN GGE has been in a state of de facto paralysis with no consensus being reached during this period; any British efforts to shape values in this regard have clearly been both under resourced and unsuccessful in achieving aims and objectives.

The Dutch *National Cyber Security Agenda*, meanwhile, is much more forthright in its declared commitment to a values driven strategy, listing its role in 'contributing to international peace and stability in the digital domain' as the second of seven priority ambitions in the Dutch agenda.[2] A core difference in comparison between the British and Dutch approaches is declared centrality in the latter's approach to interweaving values throughout its entire approach to cyber security. This comparison notwithstanding, it must be noted here that with the broader geopolitical stalemate in norms development, even the very strong Dutch approach to a values driven strategy has its limits without both broad allied adoption but also concerted actions to drive values forward.

## The data

One could be forgiven for pointing to well written national level strategies and believe that those efforts have been proven sufficient. In the case of notable incidents –such as the WannaCry and Not-Petya global attacks in 2017– national resilience models did indeed prove themselves highly capable. Despite this however, serious consideration must be paid to the fact that malevolent behaviour, whether criminally motivated or state-sponsored, continues to rise.

In establishing this, readers can easily be pointed to a bewildering array of statistical outlets to illustrate the continuing growth of cyber insecurity. This article will offer two, Accenture's *Annual Cost of Cyber Crime Study* and the British Government's *Cyber Breaches Survey*. Comparing 2017 to 2018, Accenture reported an 11% increase in security breaches among their industry respondents. Further to this was the 12% increase in the financial cost of cybercrime across those same years; in the five years

[2] National Cyber Security Centre Netherlands, CSC-NL (2018), 'National Cyber Security Agenda: A cyber secure Netherlands', p. 7, https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda.

from 2013 to 2018, these are cumulative –and staggering– increases of 67% and 72% respectively.[3]

Meanwhile, in the UK the Department for Culture, Media, and Sport (DCMS), provided intriguing statistics regarding the breadth of victims across UK business. In their *Cyber Breaches Survey* a whole 43% of UK businesses –regardless of industry, size or turnover– had detected an active cyber-attack within the previous 12 months. Added to that was a response of 75% of respondents who had received malicious phishing emails.[4]

Such numbers are compelling in revealing a picture of cyberspace as an environment rife with criminality. Fundamentally, it is clear that for all the efforts at establishing resilience at the national level, the scale of the problem posed by cybercrime has not only not been tamed but continues to grow at alarming rates in volume and cost. All of this together raises an intractable problem: national cyber resilience is a *necessary* but not *sufficient* condition in achieving a safe and secure cyberspace.

## The geopolitical picture

While the heady days of the post-Cold War liberal optimism are certainly over, it is necessary to briefly revisit them in order to reveal how we have reached the levels of insecurity today. The rise of cyberspace was grounded fundamentally in the maturation of three key technologies –the personal computer, the shared protocols for information in TCP/IP and DNS, and the World Wide Web. The explosion of the internet was seen as an inherently liberating tool, one that did not carry the need to establish any form of true political governance. One need only look to Barlow's 1996 "declaration" on the independence of cyberspace to reveal how some viewed the romanticised, apolitical view of the Internet's potential.[5]

Instead, governance was taken forward primarily as a technical practice, it was, in effect, politically agnostic for a time. Yet the fact that this was so was not down to any inherent libertarian idealism, but rather the result of historical coincidence, where technological maturation coincided with the end of the Cold War and the victory of the liberal political order. As this author has argued elsewhere, political governance was not established over cyberspace partly because without any form of political challenger, it was simply believed it did not need it.[6] The passage of events however –with our nations and the lives of citizens now intimately invested in these technologies– have since mandated the issue as a serious security concern, one that strategies and legislations have scrambled to catch up with. This has placed the liberal order at a distinct disadvantage given the evolution of the geopolitical landscape.

[3] Accenture (2019), 'Ninth Annual Cost of Cybercrime Study', March 6, pp. 10-11, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

[4] Department for Digital, Culture, Media and Sport, DCMS, United Kingdom (2019), "Cyber Security Breaches Survey 2018", https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

[5] John Perry Barlow (1996), "A Declaration on the Independence of Cyberspace", February 8, https://www.eff.org/cyberspace-independence.

[6] Danny Steed (2019), *The Politics and Technology of Cyberspace,* Abingdon, Routledge, Ch. 1.2.

Long have the arguments persisted about the decline of the Western liberal order. Mearshimer believed the liberal order's hegemony as 'destined to fail'[7] with international realities now revealing 'cracks in the liberal edifice'[8] that need to be tempered. Following in the same vein, Luce notes a fundamental 'retreat' of Western liberalism, arguing that the West is facing a crisis that 'is real, structural, and likely to persist.'[9] Emmott also follows suit in stating that 'a battle of ideas' is underway in the West[10] that parallels the positions established by Mearsheimer and Luce.

The growing, indeed burgeoning literature that has emerged dissecting the fate of the liberal order, combined with the realities of the challenges posed by areas such as fake news, serve to illustrate a key problem that has yet to be recognised in western policy circles. This problem is a fundamental crisis of confidence throughout the liberal West; a lack of faith in fundamental values that has implicitly infected the ability of Western nations to drive liberal values into the governance of cyberspace. If a liberal hegemony is under strain and challenge as Mearsheimer suggests, then other have clearly moved into the battleground in cyberspace.

## Cyber sovereignty

The rise of the challenge from cyber sovereignty has created a strong need for values assertion in future cyber security strategies. With the fundamental logic of cyber sovereignty being centred on each state retaining absolute authority over its cyberspace, those who call for this position are arguing against the establishment of values and norms behaviour. Chinese premier Xi Jinping's remarks at the 2015 World Internet Conference serve as the clearest indication of the challenge to any Western view of a free and open Internet. By stating that "We should respect the right of individual countries to independently choose their own path of cyber development…'[11]

Cyber sovereignty represents, essentially, a clear and present challenge to any notion of a values-based, open cyberspace. It determines that state sovereignty should be absolute, abiding in non-interference not only in a state's internal activities in the digital space, but complete non-judgement in the choice of any state as to how it manages its cyberspace. Such a position is a key reason for the lack of international consensus on how to govern cyberspace in the future, and why current national level cyber strategies find themselves unable to achieve their aims. So long as the international vision for the future of cyberspace itself is contested, any strategy aiming only at resilience will find itself in a purely reactive manner.

[7] John J. Mearsheimer (2018), *The Great Delusion: Liberal Dreams and International Realities,* New Haven, Yale University Press, p. 11.
[8] Ibid, ch. 4.
[9] Edward Luce (2017), *The Retreat of Western Liberalism,* New York, Atlantic Monthly Press, p. 28.
[10] Bill Emmott (2017), *The Fate of the West: The Battle to Save the World's Most Successful Political Idea,* New York, Public Affairs, p. 467.
[11] Xi Jinping (2015), Opening ceremony of the Second World Internet Conference, December 16, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

A key battleground in how sovereignty is being asserted across cyberspaces lies in the establishment of data localisation laws worldwide. With the pernicious challenges of cybercrime and attribution, states rightly recognise that in order to ensure law and order, as well as the pursuit of justice following a crime, they must be able to gather digital evidence. This very reasonable position does, however, enjoy a highly varied interpretation of applying sovereignty.

The Vietnamese 2018 *Cybersecurity Law* mandates not only that big tech firms –such as Facebook– retain their data within Vietnam, but also maintain a manned office presence within the country as well. The British 2016 *Investigatory Powers Act* also interprets sovereignty based on the location of housed data, compelling all Internet Service Providers to retain records for 12 months. This is intended to enable retrospective collection and analysis under warrant if needed for investigation.

Russia, meanwhile, carries a far more expansive view of sovereignty than most with their data localisation law, Federal Law No. 242-FZ, which requires all providers and managers of data to repatriate data on Russian national anywhere in the world back to storage in Russia itself. This law in effect declares digital sovereignty not over data, but over any individual Russian, regardless of where they are in the world. Disputes over the ethics of the law led to a ban on LinkedIn from being able to operate within Russia at all in 2016 due to their unwillingness to comply with such regulation. The Russian regulator, the *Roskomnadzor*, glibly stated that the company's refusal to comply confirmed 'their disinterest in working on the Russian market.'[12]

## Building values-driven strategies

The hope by this stage has been to establish that the vision of a free and open internet, carrying liberal values in its core DNA, is under severe political challenge. What today certainly appears as utopian times for the internet in those early post-Cold War years – where a free and open internet seemed the epitome of the liberating promise of technology– is indeed very different to the realities of today's cyberspace.

The onslaught of cybercrime and cyber espionage, as well as the experimental actions of states themselves with cyber warfare methods, have all served to destabilise a space shared by all. Cyber *in*security has become the norm, and former President Barack Obama's view that cyberspace had become a sort of 'wild, wild west'[13] remains not only true, but all available data indicates that the problems have only worsened since by volume, impact, and cost.

Not only have criminal, espionage, and acts of warfare destabilised cyberspace, they have also contributed to normalising insecurity in an environment that leads to a fundamental political challenge of the values that underlie it. Such rife and uncontrolled

[12] The Federal Service for the Supervision of Communications (2017), "LinkedIn Refused to Eliminate Violations of Russian Law", *Information Technology*, March 7, https://rkn.gov.ru/news/rsoc/news43486.htm.
[13] Barack Obama (2015), Remarks at the Cybersecurity and Consumer Protection Summit, February 13, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

conditions raise a fundamental question, "why should this space be trusted?". The pervasiveness of such insecurity combined with emerging norms of state-sponsored bad behaviour and wanton criminality places a firm question mark against the ability of foundations built on liberal values to deliver a safe and secure space for users.

In turn, this has created the opportunity for political challenge to emerged, which of course has in the form of Cyber Sovereignty. This view is gaining traction less because of its inherent political appeal, but rather because it presents a political case for how to secure the internet based on national authority. Such a case has not only not been built by Western liberal nations and, as demonstrated through even just two example national strategies above, enjoys little practical unity among allies in rhetorical construct and by actions.

It is clear that the current construct behind national cyber security strategies carries a significant flaw, which is an over-dominance of technical concerns on resilience, and a lack of focus and action on the place of values. For any strategy to not only begin protecting the nation it serves, but also to actively contribute towards stabilising the geopolitical conditions of cyberspace itself, values assertion must be considered.

To achieve this, two principles should be followed in order to bridge the gap between rhetoric and actions on values. First, there in the next iterations of each Western liberal nation's cyber security strategy should be a declared acknowledgement of a contrarian political position to the liberal vision of a free and open internet. Cyber Sovereignty should be called out as a strategic competitor that is to be resisted by all who wish to preserve and nurture cyberspace in its current form. Cyber Sovereignty has, in effect, been allowed to gain political traction due to the lack of moral and political consensus among and within Western liberal nations. A first step in aligning an alliance position should begin with this explicit declaration, which will serve to focus diplomatic efforts accordingly.

Secondly, bad behaviour in cyberspace should be called out. Much akin to how human rights organisations routinely highlight abuses and transgressions for public dialogue, bad behaviour that undermines desired norms, standards, and values should be called out. Joel Rogers de Waal words this best in saying that in any kind of information war the West should seek to 'weaponise embarrassment' as much as possible. De Waal sagely establishes that 'if liberal democracy holds unique vulnerabilities to the social media age, then so does autocracy in its existential fear of embarrassment.'[14]

De Waal's argument can be seen as proven true in the recent Iranian reaction to the shooting down of Ukranian International Airlines Flight PS752 in January 2020, where originally Iran claimed the incident an accident before confession that it had indeed shot the airliner down. This led to uproar within Iran itself as well as significant embarrassment with, and condemnation by, the international community. Such as example serves to highlight words from an unexpected source, Sacha Baron Cohen, normally known for his

[14] Joel Roger de Waal (2019), "The West Should Weaponise Embarrassment in the New Information Wars", *RUSI Commentary*, April 26, https://rusi.org/commentary/west-should-weaponise-embarrassment-new-information-wars.

comedic work, who recently gave an impassioned speech about safety and freedom on social media, making a very prescient point about the difference between democracy and autocracy: 'Democracy, *which depends on shared truths*, is in retreat, and autocracy, *which depends on shared lies*, is on the march.'[15] Recent events in Iran serve to reveal how autocracies, the driving force behind cyber sovereignty, seek to create a shared lie, and what can happen when that lie is exposed and a shared truth is established.

The same hope must be held for driving values in cyberspace, the establishment of shared truths across an environment to prevent these technologies from becoming tools of oppression concealed behind an absolute interpretation of national sovereignty. A key measure in driving the Western vision to maintain and improve a free and open internet will lie fundamentally in calling out bad behaviour at every possible turn.

## Conclusions

To conclude, this article has established a flaw at the heart of national efforts to create effective national cyber security strategies. While very successful in many regards, those strategies have fallen prey to becoming overly focused on measures of technological resilience, making them inherently reactive strategies. What has also been established is that the geopolitical environment in which these strategies operate puts a reactive strategy at a severe disadvantage, particularly in cyberspace where, as voluminous data sets reveal, cyber insecurity continues to grow at alarming rates.

National cyber security strategy constructs in their present form may deliver good performing levels of national resilience, but they have been proven unsuccessful in shaping the international dynamics in ways desirable to liberal Western nations. A core omission has been the place of values; while rhetoric can be found in many documents declaring support for values, what is missing is tangible action and alignment with allies to operationalise values into a collective allied moral position on the future of cyberspace.

By calling out Cyber Sovereignty as a challenger in future strategies, and taking concerted, allied, and regular actions to call out bad behaviour, the liberal West will begin to challenge actors who wish to shape cyberspace in their image, for autocratic purposes at odds with the original vision for cyberspace. For the vision of a free and open internet to endure, all liberal nations must recognise that the articulation, inclusion, and deployment of values must lie at the heart of all future national cyber security strategies.

[15] Sacha Baron Cohen (2019), "Read Sacha Baron Cohen's Scathing Attack on Facebook in Full: 'Greatest Propaganda Machine in History'", *The Guardian* UK, November 22, Italics added, https://www.theguardian.com/technology/2019/nov/22/sacha-baron-cohen-facebook-propaganda.