Five tests for risk-based approaches to national cybersecurity in resource-constrained environments

Digital Pathways Paper Series
DOI: https://doi.org/10.35489/BSG-DP-WP_2022/05

Ciaran Martin *and* Noran Shafik Fouad

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Digital Pathways at Oxford

Ciaran Martin, *Professor of Practice in the Management of Public Organisations;*
and Noran Shafik Fouad, *Research Associate, Digital Pathways at Oxford*

both at *Blavatnik School of Government, University of Oxford*

Paper 19
March 2022

Digital Pathways at Oxford is a research programme based at the Blavatnik School of Government, University of Oxford. It produces cutting-edge research across the fields of public policy, law, economics, computer science, and political science to support informed decision-making on the governance of digital technologies, with a focus on low- and middle-income countries.

This paper is part of a series of papers on technology policy and regulation, bringing together evidence, ideas and novel research on the strengths and weaknesses of emerging practice in developing nations. The views and positions expressed in this paper are those of the author and do not represent the University of Oxford.

Citation:
Martin, C. & Shafik Fouad, N. (2022). *Five tests for risk-based approaches to national cybersecurity in resource-constrained environments.* Digital Pathways at Oxford Paper Series; no. 19. Oxford, United Kingdom

https://www.bsg.ox.ac.uk/research/research-programmes/digital-pathways

@DigiPathOxf
Cover image: © Shutterstock

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Digital Pathways at Oxford

Table of Contents

1. Introduction

Cybersecurity has emerged as a principal concern for governments in the 21st century. The increasing cyber dependencies and the massive development of information and communication technologies (ICTs) have widened the scope of potential vulnerabilities that can be exploited in cyber incidents;[1] lowered entry barriers for potential threat actors by decreasing the costs of malicious cyber operations;[2] and in some (but by no means all) environments, created concerns that cyber offence has been prioritised over cyber defence.[3] In many political discourses, cyber threats have long been accompanied by fears of a 'cyber catastrophe' that would threaten the stability of nations, particularly when critical national infrastructures (CNIs) are attacked. Cyber Pearl Harbour, Cyber Katerina, and Cyber 9/11 are all examples of futuristic cyber doom scenarios that many governments, particularly in the global North, have been using since the 1990s in framing cybersecurity threats as part of the realm of national security.[4] As argued by Lee and Rid, the hype and fear around destructive cyber attacks had immunised cybersecurity budgets from the sorts of severe reductions in national security spending seen in the post-financial crash years.[5] In part, this is because investment in covert intelligence to detect and counter the most sophisticated threats is deemed by many security leaders as an essential part of the solution to the cybersecurity challenge.

Further, tough standards are demanded to protect CNIs, even if those standards are not always met. Governmental guidance to mainstream cybersecurity for public services, smaller businesses, or charitable organisations seems to recommend very advanced and expensive defences. As part of this process, institutional capacity for cybersecurity has been hugely strengthened in many countries. The USA, for example, has several very large security agencies – the National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) – with advanced cyber expertise. The UK led the other so-called 'Five Eyes' intelligence alliance – the UK, USA, Canada, Australia and New Zealand – in setting up intelligence-led but civilian-facing cybersecurity authorities with costly technical capabilities. Much of continental Europe introduced a blend of covert intelligence agencies and separate, public-facing, cybersecurity authorities.

Such ideas, policies and institutions, which are primarily influenced by the experiences of the most advanced economies and powerful states, have largely shaped what national-level cybersecurity should look like. This has created a situation where countries that manage to develop their financial and technical capacities and transition into the status of 'emerging economies' invest heavily in militarising their cybersecurity strategies. For example, emerging economies such as Argentina, Brazil, Indonesia, Philippines, Mexico, and South Africa have all either already established or are in the process of establishing specialised military agencies for cybersecurity, that is, cyber

[1] Geers, K. (2011) *Strategic Cyber Security*, 117.

[2] Weinstein, D. (2014) Snowden and U.S. cyber power, *Georgetown Journal of International Affairs*, 4:4-11.

[3] Rattray, G.J. (2009) An environmental approach to understanding cyberpower, in Kramer, F.D., Starr, S.H. and Wentz, L.K. (2009) eds *Cyberpower and National Security*. Dulles, VA: Potomac Books, Inc., 272.

[4] Sean T. Lawson, S.T. (2019) *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. New York: Routledge.

[5] Lee, R.M. and Rid, T. (2014) OMG cyber!: Thirteen reasons why hype makes for bad policy, *The RUSI Journal* 159, no. 5: 4–12.

commands.[6] This increasing role of military and intelligence agencies in cybersecurity around the world has been criticised extensively by cybersecurity scholars for various reason, including: the negative implications of militarisation on digital human rights and internet freedoms which transform activists into 'cyber losers';[7] the atmosphere of insecurity and tension it creates in international relations;[8] and the challenges it poses to democratic governance in fragile political settings.[9]

Here, one important question remains largely under-explored: **what cybersecurity requirements should countries with limited economic resources consider for digitalisation to improve public services and create the conditions for further economic growth?** Put differently, **what does good, cost-efficient, and economically viable national cybersecurity look like?** There is little evidence available to help answer this question, and this is clearly an area where detailed quantitative research would be beneficial.

The nascent attempts to rank global cybersecurity efforts between countries further illustrate this point. Rankings vary wildly between the different indexes, which shows that the world is unable to measure cyber harm, and is nowhere near an agreed way of assessing what good cybersecurity looks like. For example, the International Telecommunication Union (ITU) ranks China 33rd in its Global Cybersecurity Index,[10] whereas Harvard's Belfer Center's National Cyber Power Index ranks the same country second.[11] Estonia's National Cyber Security Index ranks Greece first in terms of preparedness to prevent cyber threats and manage cyber incidents,[12] but Greece does not appear highly in any other major index. This is partly due to the very different methodologies these indexes use. For example, the ITU's index focuses heavily on governance: national strategies, incident response capabilities, legal measures to regulate cybersecurity, etc, whereas the Belfer Center's index measures countries' observed behaviour towards cyber issues to achieve certain objectives, as well as the quality and quantity of output to achieve them (such as the number of patents filed per year, global top security firms, skilled workers, etc).

While we cannot currently accurately specify what good cybersecurity looks like, we can analyse what good risk-based approaches to national cybersecurity should aim at achieving. This is particularly important in low- and middle-income countries operating in resource-constrained environments in the early stages of economic development and digitalisation. This paper, therefore, discusses key considerations for risk-based cybersecurity by investigating the trade-

[6] Solar, C. (2020) Cybersecurity and cyber defence in the emerging democracies, *Journal of Cyber Policy* 5, no. 3: 392–412.

[7] Brantly, A.F. (2014) The cyber losers, *Democracy and Security* 10, no. 2: 132–55.

[8] Cavelty, M.D. (2012) The Militarisation of Cyberspace: Why less may be better, in *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. Institute of Electrical and Electronics Engineers (IEEE), 1–13 [online] Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243971.

[9] Solar, C. (2020) Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, 5:3, 392-4.

[10] ITU (2021) *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity* [online] Available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

[11] Voo, J. et al. (2020) *National Cyber Power Index 2020*. Harvard Kennedy School, Belfer Center for Science and International Affairs. [online] Available at: https://www.belfercenter.org/publication/national-cyber-power-index-2020

[12] e-governance Academy (n.d.) *National Cybersecurity Index* [online] Available at: https://ncsi.ega.ee/ncsi-index/?order=rank

offs that decision-makers should address so that scarce resources are best deployed to fend off threats that are more likely to happen and cause significant harm. The analysis is presented in the form of **five tests** that can be used to analyse the robustness of risk-based cybersecurity when resources are limited and to think about the potential paths that nations can take as they grapple with various economic and digitalisation challenges. As such, this framework does not present an exhaustive list of all the fundamental components of a cybersecurity strategy, but rather analyses the most important trade-offs and challenges that a cybersecurity strategy should address.

Test 1: A robust and realistic assessment of hostile state cyber operations and likely intent

One of the most corrosive myths in cybersecurity is that hacking is so easy that lethal force can be deployed in cyberspace by almost anyone. The image of a teenager in a hooded top causing devastation from a suburban bedroom has become ubiquitous in the depiction of cyber conflict. However, the reality is much more complex. It is indeed very easy to acquire basic hacking tools and capabilities, but the power to carry out destructive cyber attacks is highly specialised and so mostly available to a small number of capable state actors. Developing destructive cyber capabilities requires a huge amount of money, skills, infrastructure, stable operating environment, and time – that is, it requires the backing of a competent nation state. That is why, despite earlier hype to the contrary, terrorist organisations have never managed to acquire or deploy the sort of destructive cyber capabilities they would no doubt be willing to deploy.

In assessing the risk of a wide-scale disruptive or potentially destructive cyber attack, states need to consider the cases of offensive cyber attacks to date (especially against small or middle powers), the actors behind them, their motives, as well as the link between these cases and any pre-existing geopolitical, economic, or political rivalries. For example, the Stuxnet worm, first publicised in 2010 – widely believed to be a highly targeted Israeli and US cyber operation to degrade the capabilities of the Iranian nuclear centrifuges in 2010 – is an example of an offensive cyber operation that is tied to political and strategic rivalries.[13] Russia's use of similar highly disruptive cyber operations against less-powerful countries has been mostly tied to direct military conflict or tensions short of military conflict. For example, Georgia suffered serious cyber attacks from Russia during the war of 2008,[14] and again in 2019 when much of the Georgian Government's web presence was taken offline.[15] Ukraine has seen repeated disruptive intrusions on its digital infrastructure, with the most serious cases peaking around the Crimea crisis of 2014; in December 2015, when hackers compromised the information systems of three energy distribution companies in Ukraine;[16] and most recently after the Russian invasion in 2022, though perhaps not on the scale many would have predicted would accompany a full-scale invasion of the country.[17] Geopolitical rivalries also motivated the Iranian regime in 2012 to launch the so-called Shamoon virus to attack the servers of Saudi Arabia's national oil company, Aramco, erasing up to 32,000 hard drives and causing huge disruption.[18]

[13] Lindsay, J.R. (2013) Stuxnet and the limits of cyber warfare, *Security Studies* 22, no. 3: 365–404.

[14] Gamreklidze, E. (2014) Cyber security in developing countries, a digital divide issue', *The Journal of International Communication* 20, no. 2: 200–217.

[15] Winder, D. (2019) Georgia 'I'll Be Back' cyber attack terminates TV, takes down 15,000 websites, *Forbes*, sec. Cybersecurity [online] Available at: https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites.

[16] Geers, K. ed. (2015) *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 103–111.

[17] Martin, C. (2022) Cyber Realism in a Time of War. *Lawfare* [online] Available at: https://www.lawfareblog.com/cyber-realism-time-war

[18] Bronk, C. and Tikk-Ringas, E. (2013) The cyber attack on Saudi Aramco, *Survival*, 55:2, 81-96.

In global terms, these threat sources are relatively isolated. Very few countries possess high-grade cyber capabilities to launch highly disruptive or destructive attacks. Those that do rarely use them, especially in the absence of pre-existing conflicts that could create an intent to launch such attacks. There is, therefore, a risk judgement for nations to make as to whether or not to direct more of their attention and budgets to defending against a potential state-launched destructive cyber attack. It is not, of course, as simple as suggesting that if a state does not feel directly threatened by the most powerful and capable actors, it can neglect the highest end of cyber defences; there are at least two other aspects to consider. One is the attempts by an increasing number of countries to develop their offensive cyber capabilities and develop military commands, even if they have not yet demonstrated an actual intent or capacity to use them. Another is the risk of proliferation of supposedly targeted destructive attacks going wrong and spreading beyond their targets, as NotPetya and WannaCry attacks in 2017 showed.[19] Risks remain, but countries may take a perfectly realistic position and assume that the most potent nation-state threat to them is at present, and in the foreseeable future, unlikely to have the intent and capability to launch the sort of devastating cyber attack that requires the most expensive capabilities and that could cause collateral damages that affect the state that launched the attack itself.

[19] Buchanan, B. (2020) *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics,* Cambridge, MA: Harvard University Press, 280-290.

Test 2: Addressing the persistent threat of cyber espionage

Cyber espionage has become a common practice in international relations, as conventional forms of espionage always have been. It is therefore reasonable for states to assume that their governmental communications can be routinely compromised for espionage purposes, particularly by state actors that possess such capabilities. Protection against cyber espionage usually involves avoiding the use of modern technology for sensitive government communications and data, or using very sophisticated and expensive specialist tools to secure them. For that reason, some governments only use these sophisticated tools for specialised communications, normally relating to national security and diplomacy. For example, in 2012, the UK Government adopted a policy that assumed that anything classified at below 'secret' – that is, anything stored on ordinary, enterprise IT – could be compromised by a capable state actor. That does not mean that all information stored on states' computer systems would be necessarily stolen and analysed by other countries; there is far too much information to process, and a huge majority of such information will be of no interest to other countries. Nor does it mean that any and every country can routinely spy on any other. But it does mean that systematic protection against cyber espionage for most information on governments' systems is not entirely possible.

The risk assessment here should be centred around determining the specific areas of sensitivity in governments' communications and data that need special protection, either by managing them offline or by buying and operating specialist equipment to secure them. This is not always easy, however, because such equipment is expensive and also very complicated and difficult to commercialise, given that demand is sufficiently low. Hence, companies that develop such products are often subsidised, directly or indirectly, by some of the most powerful countries. This problem has recently emerged via *The Washington Post* revelation in 2020 about what was described as 'the intelligence coup of the century'.[20] This revealed how US and West German intelligence had controlled the technology of a highly successful Swiss cryptography firm, Crypto AG, which dominated the market for a range of other countries in the latter part of the Cold War. The products and services offered by Crypto AG were deliberately altered by US and West German intelligence agencies to make the traffic apparently protected but easy for them to decipher. Crypto AG's client list included most of Latin America's military juntas, India, Pakistan, Iran, and even the Vatican. Similarly, the US Government has long accused Russian firms such as Kaspersky, an anti-virus company, and the Chinese telecommunications giant Huawei, of acting as proxies for data exfiltration for their host governments. These stories illustrate the need to proceed with caution in choosing the right tools to protect the country's most sensitive information systems.

[20] Miller, G. (2020). The intelligence coup of the century, The Washington Post, 11 February 2020. [online] Available at: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Test 3: Identifying critical infrastructure and evaluating its resiliency

The third test moves away from actor-specific assessments of the motives and capabilities of other nations towards a broader one: on what infrastructure does the country most depend, and how resilient is it against cyber attacks from any actor for whatever motive? This test is also important for requiring an assessment of the impact of accidental failure, as the mitigation for both challenges – a deliberate attack or accidental failure – tends to be identical.

Critical infrastructure is usually given much attention in national cybersecurity strategies given their interaction with physical systems that, if attacked, may have a debilitating effect on national security, economic security, public health or safety. Countries differ significantly in identifying the infrastructure that matters most to them. For 'hard' infrastructure – for example, communications, transportation, or energy – some countries are entirely dependent on imports; others on locally sourced materials. For 'softer' infrastructure, such as voting, digital dependency varies: some voting systems are entirely manual and therefore largely invulnerable to cyber disruption, while others operate fully or partially online with a profoundly different risk profile. Another key difference is the degree of government ownership. Since the onset of privatisation, more and more critical infrastructure is becoming privately owned. This transfers the onus of policymaking away from direct government action towards regulators.

Regardless, a core part of any risk-based cybersecurity strategy in any nation is mapping out the infrastructure on which its vital services depend, the inter-dependencies between them, the weaknesses of resilience, and taking steps to address them accordingly. Best practices have evolved to ensure that it is not prevention of attacks that matters most, (given the ubiquity of cyber intrusions), but the ability to contain them and to mitigate their consequences. For example, no social security system can be made impervious to fraudulent online activity, but it can be configured to contain the maximum damage that can be done by a single threat actor (either an insider or a hostile outsider) in the same way as global financial institutions now have to configure their systems to limit the damage done by a rogue trader. Similarly, power grids, telecommunications exchanges, water supplies and other critically important sectors need to have procedures in place that can cope safely with the loss of some parts of critical capacity as a result of cyber attacks.[21]

There is an important distinction to be made here between cybersecurity and physical safety. Critical systems are increasingly digitised, and so are increasingly vulnerable to digital disruption via cyber operation. However, no critical system on which human safety or life depends – for example, an air traffic control system – should be *entirely* dependent on a computer system. Computer systems can fail comprehensively, by accident or as a result of a malicious operation. Therefore, a system such as air traffic control needs a safe backup operating procedure, even if this means significant disruption, delay and economic cost.

[21] For a general discussion on national cybersecurity strategies in the Global South with a specific focus on critical infrastructure, see Schia, N.N. (2018) The cyber frontier and digital pitfalls in the Global South, *Third World Quarterly*, 39:5, 821–837.

Test 4: Assessing the risk to personal and private sector data with citizen buy-in

This test is rooted in the ubiquity of cyber crimes that exploit the illicit but hugely profitable market of personal and private sector data. The experiences of many countries have shown that rapid, low-cost digitalisation of public services and the wider economy, is possible but comes at the price of endemic personal data insecurity. This challenge is one that should be addressed not just by governments, but by the whole of society. On the government side, protecting digital public services involves several key choices. The first is whether the government should build its own infrastructure or procure cloud-based services. Although moving to the cloud has implications for digital dependency (discussed further in Test 5), it is becoming more cost-effective and relatively more secure. Assuming that cloud-based services are the chosen option, governments would need to decide on their security posture. Many states insist on in-country data storage of citizens' personal data held by the government to avoid security breaches. For example, in 2017 Sweden was caught in a political scandal about a data breach at its national transportation authority. Contractors in at least two countries outside Sweden had access to population-level data which leaked,[22] and the Swedish Government was unable to account fully for its data storage location policies. As well as being more expensive, in-country data storage also places more obligations and costs in-country because of the costs it imposes on the cloud providers, given that data centres require physical protection, not just virtual protection.

There are also societal-wide choices to be made, particularly about data protection regulations and protecting citizens privacy. For example, Brazil suffered one of the largest and most detailed data breaches per capita in world history in 2021. It was not just the number of personal records that was stark – at 223 million, this is more than the official population of the country because the records of several million deceased were included in the breach.[23] More striking was the extent of the personal data that was leaked. It ranged from taxpayer registration numbers and vehicle data to credit rating assessments, among other treasure troves for the online criminal market. The country responded by introducing data protection regulations into parliament, one of the key attempts to legislate for the activities of the largely American-owned platforms. However, the reality is that attitudes to personal data privacy differ greatly across and within societies. Moreover, greater regulation may prompt higher service costs and greater complexity in service access, including for public services, placing digital inclusion agendas at risk. Few countries have reached a consensus on how to achieve the right balance.

[22] Anderson, C. (2017). Swedish government scrambles to contain damage from data breach, *The New York Times*, 25 July 2017. [online] Available at: https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html

[23] Petrov, A. (2021) Federal police arrest hacker suspected of the largest data leak in Brazil, *The Rio Times*, 19 March 2021. [online] Available at: https://www.riotimesonline.com/brazil-news/technology/fedeal-police-arrests-hacker-suspected-of-the-largest-data-leak-in-brazil/.

Test 5: Manoeuvring around great power competition

A final and crucial test is about sourcing technology and manoeuvring around the great power competition to control it. Such competition can be seen now in the debates on internet governance and China's call for a decentralised internet infrastructure and Russia's bid to duplicate it. Some studies argue that this would eventually end the multi-stakeholder management of the internet, increase states' control, and challenge cyber defence in a fragmented network, often called the 'Splinternet'.[24] The potential consequences of this so-called Splinternet is a striking feature of the discussion on digitalisation in many countries. In cybersecurity terms, while off-the-shelf technology built by superpowers has its advantages, as it needs to have good security standards to ensure commercial success, it comes at a cost of control and choice to the country that buys it. The quest for complete digital autonomy may also be long, arduous, expensive, and potentially unsuccessful.

However, this does not mean that countries cannot manoeuvre around this competition and potentially influence the future direction of the global governance of cybersecurity and internet governance. For example, India is sometimes seen as a 'swing state' that shifts support between Russia and China on one side and the USA and the EU. Rather than economic domination or spatial imperialism, its approach is based on protecting ICTs to eradicate poverty, and promoting human security, which puts it in a particularly good position in international dialogues on cybersecurity.[25] Similarly, Brazil is playing a pivotal role in the negotiations on cybersecurity and data protection, particularly around internet governance.[26] Its cybersecurity strategy is mainly linked to its economic security strategy and therefore it has been imposing high import tariffs and tax breaks to leverage domestic ICT industries.[27] Another example is South Korea, which is particularly active in debates on the applicability of international law to cyberspace, and adopting confidence-building measures for the financial sector.[28] That is, great powers are not going to be able to decide the future of the internet and the global governance of cybersecurity alone, and there exists a space of manoeuvre for small and middle powers to exert some influence on the current debates.

[24] Hoffmann, S., Lazanski, D. and Taylor, E. (2020) Standardising the Splinternet: How China's technical standards could fragment the internet, *Journal of Cyber Policy* 5, no. 2: 239–64; Claessen, E. (2020) Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: The case of Russia and the EU, *Journal of Cyber Policy* 5, no. 1: 140–57.

[25] Segate, R.V. (2019) Fragmenting cybersecurity norms through the language(s) of subalternity: India in 'the East' and the global community, *Columbia Journal of Asian Law* 32, no. 2; Ebert, H. (2020) Hacked IT superpower: How India secures its cyberspace as a rising digital democracy, *India Review* Vol. 19, no. 4: 376–413.

[26] Canabarro, D.R. and Borne,T. (2015) The Brazilian Reactions to the Snowden Affairs: Implications for the study of international relations in an interconnected world. *Conjuntura Austral, Porto Alegre*, v.6, n.30, p.50-74 [online] Available at: https://papers.ssrn.com/abstract=3155476.

[27] Kshetri, N. (2016) *The Quest to Cyber Superiority: Cybersecurity regulations, frameworks, and strategies of major economies*. Cham, Switzerland: Springer International Publishing.

[28] Ebert, H. and Groenendal, L. (2020) *Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU cooperation*. EU Cyber Direct. [online] Available at: https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/iXvfE20z/digital-dialogue-rok.pdf.

Conclusion

Extensive research and practical work has been done for cybersecurity capacity building, particularly in low- and middle-income countries. However, there are clear in-built constraints on what can be achieved with scarce resources. Hence, a first step to enable targeted capacity building is a risk assessment aimed at allowing the country to make a series of realistic choices about its digital security posture. Ultimately, the national dialogue on cybersecurity in any country comes down to two basic questions: what does this nation really care about? And how much can it afford to care about it? This paper presents a framework to dissect these questions as a basis for further discussion, and analysis of possible options for different countries to take based on their conclusions about their own circumstances.


BLAVATNIK
SCHOOL OF
GOVERNMENT
UNIVERSITY OF
OXFORD


Digital
Pathways
at Oxford