ISSUE BRIEF

JUNE 2024

The Impact of Corruption on Cybersecurity: Rethinking National Strategies Across the Global South

ROBERT PEACOCK

EXECUTIVE SUMMARY

Recent government-wide shutdowns of information systems in a half-dozen developing countries ranging from Albania to Vanuatu suggest that ransomware and state-sponsored attacks are finding success in targeting critical infrastructure networks of the Global South. Over the first decade of their integration with the digital economy low-income and lower-middle-income countries faced relatively few cyberattacks, but that honeymoon appears to be over, with the Global South now ranking first in cyberattacks per institution and cyberattacks per capita.

As mobile device e-commerce and ICT networks continue to expand across the Global South, this rise in cyberattacks is not surprising. Nevertheless, the level of digital integration in the region still trails the rest of the world, suggesting the record-setting levels of cyberattacks may be the result of vulnerabilities systemic to the region. The most corrosive of these problems is corruption. While few governments in the Global South have publicized the role of IT corruption in critical infrastructure enterprises, this analysis builds on donor and regional software association investigations to argue that IT departments in the Global South are vulnerable to corrupt procurement schemes catalyzed by the proliferation of pirated software.

Until recently the prevalence of pirated or lapsed licensed software on government networks across the Global South may have led to little more than poor or unpredictable network performance. This is no longer the case today, as networks built around pirated software serve as easy targets for ransomware gangs and hacktivists that still find decades-old malware like the “WannaCry” worm to be effective in countries challenged by systemic corruption.

In response to the growing cyber threat, governments in the region and foreign donors focused their response on the best practices found in the action plans and policy initiatives drawn from national cybersecurity strategies designed for the Global North.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

As a result, not one government's national cybersecurity strategy in the Global South recognizes corruption as an important issue for critical infrastructure network security.

This analysis underlines the effects of addressing corruption on cybersecurity by highlighting the positive impacts of Ukraine's switch to an autonomous and transparent procurement platform by comparing the experience of cyberattacks in 2017 with those that accompanied the 2022 full-scale invasion of the country. Taking these lessons forward, cybersecurity officials across the Global South must consider identifying procurement corruption as a cybersecurity risk and develop initiatives to mitigate the impact of systemic corruption on cybersecurity.

INTRODUCTION

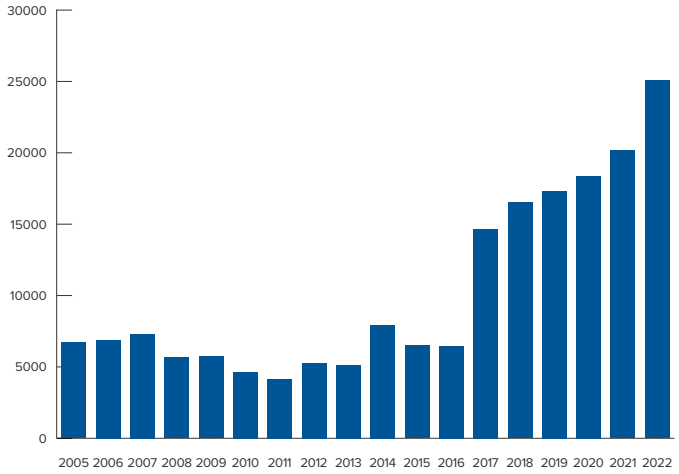
"CYBER CRIMINALS ARE COMING FOR THE GLOBAL SOUTH" – DEUTSCH WELLE [1]

The global revolution in information and communications technology (ICT) has expanded educational and economic opportunities across the Global South[2] even as it brings new threats of inequality and cyber vulnerability. Whether these countries are prepared, they now represent the fastest-growing population of new internet users. Moreover, malicious hackers have recognized this rise in networked users, with Latin America and the Caribbean now leading the globe in the rate of cyberattacks as a share of the networked population,[3] while Africa leads in the rate of cyberattacks per institution.[4]

The process of digital transformation started later in the Global South, which likely limited the vulnerability of these countries to ransomware attacks. This is no longer the case. Vanuatu served as a wake-up call in 2022 when most of the island's public services shut down after hackers encrypted the government's data networks.[5] The ransomware gang's commitment of time and resources to infiltrate Vanuatu's government networks demonstrates that even the smallest nations in the Global South can no longer assume they will be overlooked by global hacker organizations.

A critical lesson from the first decade of ubiquitous cyberattacks is the importance of patching an enterprise's network software. Unfortunately, the vulnerabilities that IT professionals must track and patch each year have been growing, especially since the arrival of cryptocurrency in the mid-2010s offered the first practical means for hackers to receive payments after locking up or seizing data.[6] Figure 1 shows MITRE's recorded annual increase in registered vulnerabilities and exposures, which shows the growth has been rising at an exponential rate since 2018. As ransomware began to grow and criminal organizations sought to continue finding lucrative and vulnerable targets, hackers suddenly turned to institutional networks in countries they might never have heard of before researching potential targets.[7] A growing horde of ransomware organizations appear to be choosing targets based first on vulnerability, which has resulted in more attacks on institutions in the Global South.[8]

Figure 1: New IT Product and Service Vulnerabilities



DATA SOURCE: MITRE

1 Janosch Delcker, "Ransomware: Cyber criminals are coming for Global South," *Deutsch Welle*, August 28, 2022, https://www.dw.com/en/ransomware-cyber-criminals-are-coming-for-the-global-south/a-62917234.

2 Although the term Global South is a preferred term for those nations most challenged in economic growth and good governance, there is no set definition of its membership. This policy brief defines the Global South not by geography or GNP, but rather by any country that is not one of the top 60 countries in Transparency International's Global Corruption Perceptions Index (CPI). Therefore, geography is not the defining feature that explains why Uruguay (Latin America's richest country and 14th ranked by the CPI index) is defined as Global North while Hungary is not.

3 Charlette Donalds, Corlane Barclay, and Kweku-Muata Osei-Bryson, *Cybercrime and Cybersecurity in the Global South*, (London: Taylor & Francis, Routledge, 2022).

4 "Global Cyberattacks Continue to Rise with Africa and APAC suffering most," *Checkpoint Research*, April 27, 2023, https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/.

5 Nabilah S., "The Vanuatu ransomware attack serves as a warning to others," *TechinPacific*, May 2023, https://www.techinpacific.com/the-vanuatu-ransomware-attack-serves-as-a-warning-to-others.

6 Nikhilesh De, "State of crypto: Ransomware is a crypto problem," *Coindesk*, February 10, 2022, https://www.coindesk.com/policy/2021/06/08/state-of-crypto-ransomware-is-a-crypto-problem/.

7 Sheera Frenkel, "Hackers find 'ideal testing ground' for attacks: Developing countries" *The New York Times*, July 2, 2017, https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html.

8 Jai Viljayan, "Majority of ransomware attacks last year exploited old bugs.," *Dark Reading*, February 20, 2023, https://www.darkreading.com/cyberattacks-data-breaches/dozens-of-vulns-in-ransomware-attacks-offer-adversaries-full-kill-chain.

Although the need to patch software vulnerabilities has never been higher, corrupt practices in software procurement explain why many organizations do not regularly update their security. Functioning software that was not legitimately acquired rarely provides a connection to the software vendor.[9] The presence of pirated software on a network reduces the likelihood that the network is regularly receiving updates that the software's producer distributes to patch newly discovered vulnerabilities.[10]

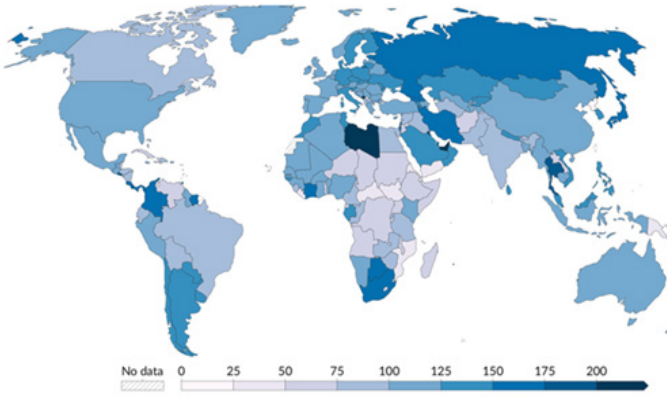
An organization's cybersecurity can also face vulnerabilities due to obsolete versions of software still running on its network. This can happen for multiple reasons, from vendors going out of business to developers choosing to no longer support a product line. In underfunded institutions across the globe, it is not rare to find the continued use of obsolete software. This vulnerability is further exacerbated by procurement managers prioritizing corrupt rents over issues of trusted vendors or sustainable support for software.

Given the epidemic levels of corruption in public and private procurement across the Global South,[11] this study draws from recent cybersecurity experiences in European and Eurasian economies similarly challenged by corruption to argue that a digitally integrated Global South may be more susceptible to cyberattacks than those in the Global North. While the limited scale of the digital economy across most of the Global South continues to keep these countries out of top spots in terms of the total number of attacks, the Global South has suddenly become a disproportionately high malware target.[12] This new reality reflects unique challenges to cybersecurity in the Global South and also suggests that the solutions to this challenge may not be found in the traditional national cybersecurity strategies based on the playbooks of more developed countries.

THE DIGITALIZATION OF THE GLOBAL SOUTH HAS ONLY BEGUN

The International Telecommunication Union estimates that the Global South passed the milestone of more than half of its citizens gaining access to the internet in 2022. At this growth rate, more than 75 percent of the Global South will be connected by the end of 2025.[13] Most of this access is represented by limited bandwidth connections to mobile phone subscribers, which allow for a range of services to citizens that, because of resource constraints or great distances, were previously impractical to offer at scale. For example, the tiny nation of Vanuatu provides its citizens residing across its far-flung islands the ability to use mobile phones to pay utility bills and taxes or initiate government document requests without a long trip between islands.[14] The economic impact is enormous for citizens who are no longer required to spend 1-2 days of travel for administrative tasks.

Figure 2: Mobile Phone Subscriptions in 2022 by Population



SOURCE: OUR WORLD IN DATA (WORLD BANK DATA)

The private services offered by early mobile phone entrepreneurs in the Global South have been no less impressive. Widespread mobile phone use looks to be a pathway from poverty for millions of citizens once isolated from the global flow of information resources.[15] ICT-based businesses may already be the leading force for economic growth in many of these countries. A study between 2007 and 2016 found mobile phone diffusion had a more significant impact on the rise in gross national product (GNP) in Sub-Saharan Africa than any other form of investment.[16] Across Africa, rural residents who lack access to landline phones or banks benefit from nearly one billion mobile phones that allow them to tap into the internet sites (notably, banking and wholesale services) necessary to engage in entrepreneur-

9 Paul Tassi, "Why Microsoft is giving away Windows 10 to Pirates," *Forbes*, March 19, 2015, https://www.forbes.com/sites/insertcoin/2015/03/19/why-microsoft-is-giving-away-windows-10-to-pirates/?sh=51c6e4ae712f.

10 Victor DeMarines, "Look before you click: The risk of buying pirated software," *Revenera*, January 17, 2020, https://www.revenera.com/blog/software-monetization/look-before-you-click-the-risk-of-buying-pirated-software/.

11 Sope Williams-Elegbe, "Systemic corruption and public procurement in developing countries: are there any solutions?," *Journal of Public Procurement* (2018) vol. 18, no. 2, 131-147, https://doi.org/10.1108/JOPP-06-2018-009.

12 "Global Cyberattacks Continue to Rise with Africa and APAC suffering most," *Checkpoint Research*.

13 "Global Connectivity Report 2022, ITU, 2022, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022.

14 "John Jack," E-governance in Vanuatu: A whole-of-government approach," *Asia Pacific Journal of Public Administration* (2018), https://www.tandfonline.com/doi/abs/10.1080/23276665.2018.1545354.

15 Valentina Rotondi, "Leveraging mobile phones to attain sustainable development," *Proceedings of the National Academy of Sciences*, June 1, 2020, https://www.pnas.org/doi/full/10.1073/pnas.1909326117.

16 Raif Bahrini, and Alaa A. Qaffas, "Impact of information and communication technology on economic growth: Evidence from developing countries," *Economies* (2019), vol. 7, no. 1, https://www.mdpi.com/2227-7099/7/1/21.

ial activity.[17] Moreover, the nascent digital information space in these countries has allowed the emergence of internet-based businesses specifically supporting rural entrepreneurs with a range of supply chain and logistic services.[18]

Despite the rapid growth in mobile phone-led economic activity, most countries in the Global South are just now starting to develop the ICT infrastructure needed to support this demand. Many states in the Global South have only completed the "first mile" of broadband access–global connections to their capitals and large cities–and large parts of the population still lack access to reliable broadband internet[19] Like mobile phone connectivity, widely distributed broadband is positively associated with economic growth. Two findings have become measuring sticks in the digital development sphere: the World Bank estimates that a 10 percent increase in broadband leads to a 1.4% increase in GNP[20] and the McKinsey Global Institute found ICT economic activity over the first decade of internet connectivity may have accounted for more than 21% of the gross domestic product (GDP) growth in mature economies.[21]

The new wave of ICT development in the Global South is realizing this economic potential by bringing broadband infrastructure to smaller cities and rural communities. Improved connectivity is already affecting the quality of life in the Global South,[22] allowing for national e-business, good governance solutions, and social services like healthcare and education to operate beyond the limited bandwidth offered by mobile phone data connections.

The World Bank has provided more than $1.2 billion in ICT lending alone for broadband development in Africa, the South Pacific, and the Caribbean.[23] Moreover, Nigeria and Mozambique have led the way in Africa by licensing SpaceX's Starlink service, which offers near broadband connections through low-orbit satellites for private users.[24] Certainly, Starlink's fees and terminals are barriers to access for most citizens in the Global South, but it and future providers are the first competitors to largely state-owned services in the region that have not succeeded in providing economical and reliable high-speed service across large swaths of territory.

Nevertheless, the growing benefits of the information age in the region come with risks–this same connectivity also attracts scores of cyber criminals who expect to profit from vulnerabilities in connected enterprise networks.

CORRUPTION IN PUBLIC PROCUREMENT

Corruption in procurement processes is a global problem, but the scale of systemic corruption in procurement tenders in the Global South has long been a major obstacle to developing effective governance and prosperity.[25] This issue does not go unrecognized by local leaders and external advisors, but they rarely account for this threat when drafting new regulatory or development initiatives.[26] The backroom decisions on what hardware and software is purchased for large enterprise information networks may be the archetype of systemic corruption but it is routinely missed by national cybersecurity strategists.

As with most forms of corruption, there are few studies on corrupt practices in software procurement but countless anecdotes of rent-seeking found in public sector network management in developing countries.[27] In this author's thirteen years of experience overseeing IT development projects in four post-Soviet countries in Europe and Eurasia, this was the common view of corruption held by those working for critical infrastructure enterprises and IT Departments inside and outside government. Control over IT procurement decisions in systemically corrupt countries is ideally suited for inflating costs and hiding kickbacks because networks are built around software that is neither visible

17 Andrea Willige, "Here's Why Africa is the World Leader in Digital and Mobile Banking," World Economic Forum, November 21, 2023, https://www.weforum.org/agenda/2023/11/africa-digital-mobile-banking-financial-inclusion.

18 Raif Bahrini and Alaa A. Qaffas, "Impact of information and communication technology on economic growth."

19 Laura Wood, "The future of African fiber markets 2023," *BusinessWire*, June 15, 2023, https://www.tandfonline.com/doi/abs/10.1080/23276665.2018.154535.

20 *Extending Reach and Increasing Impact: Information and Communications for Development*, World Bank, 2009, https://documents1.worldbank.org/curated/en/645821468337815208/pdf/487910PUB0EPI1101Official0Use0Only1.pdf.

21 Ankit Fadia, Mahir Nayfeh, and John Noble, "Follow the leaders: How governments can combat intensifying cybersecurity risks," McKinsey & Company, September 16, 2020, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks.

22 Temitaya Jalyeola, "73% Africans in rural areas lack internet access," *Punch*, December 19, 2022, https://punchng.com/73-africans-in-rural-areas-lack-internet-access.

23 World Bank Data – Vanuatu, The World Bank, 2020, https://data.worldbank.org/country/VU.

24 Jason Rainbow, "Starlink approved in Nigeria and Mozambique, says Elon Musk," *Spacenews*, May 27, 2022, https://spacenews.com/starlink-approved-in-nigeria-and-mozambique-says-elon-musk/.

25 Jens Ivo Engels, "Corruption and anticorruption in the era of modernity and beyond" in Ronald Kroeze, Andre Vitoria, G. Geltner (Eds.), *Anticorruption in History*, (Oxford: Oxford University Press, 2018).

26 Sandipto Dasgupta, "The power of corruption," *Comparative Studies of South Asia, Africa, and the Middle East* (2019), vol. 29, no. 3, https://doi.org/10.1215/1089201X-7885524.

27 Dante Deo, "Mega millions lost to software procurement fraud and error," *ITWeb*, May 9, 2023, https://www.itweb.co.za/article/mega-millions-lost-to-software-procurement-fraud-and-error/KBpdg7pmNKjMLEew.

nor readily measurable as authentic through the standard procurement oversight measures of quantity, delivery, and price.[28]

Another barrier to changing the software procurement culture in the Global South is the social norms and expectations among senior management and network administrators who in their everyday lives use or interact with pirated software on personal devices.[29] In countries where the use of pirated software is not viewed as a significant ethical or technical issue, managers of critical infrastructure enterprises may be less hesitant to acquire cheaper, pirated software for their networks. In fact, this may even be perceived as a positive decision that reduces the organization's IT budget.

The Business Software Alliance (BSA) found that although globally one-third of software in the private sector is unlicensed, in countries in the Global South this proportion may be twice as high. In the last breakdown for the Middle East and Africa in 2019, for instance, the BSA found that fifty-six percent of software in use was pirated.[30] This short-sighted view of the risks of pirated software undermines the state's ability over the long term to protect domestic networks from cyberattacks. While most government officials in the region were raised in a previous era of altruistic websites distributing unlicensed software with few downsides, this is no longer the case. One of the few studies examining pirated software samples from eleven developing countries found that 61 percent contained malware.[31]

The illicit rents found in legal software procurement, on the other hand, come in the form of bribes paid to one or more employees at the purchasing firm, an intermediary, or the supplier. This can occur through the purchasing enterprise soliciting the bribe (extortion), the seller offering the bribe for colluding (kickback), or an intermediary receiving fees or commissions on the inflated price of the transaction.[32] Interviews with investigators of private procurement fraud in the Global South find that most align with the dominant embezzlement practices found in the country's wider economy.[33] As the seller can often procure pirated or unsupported software at a fraction of the market price, the rents gained by the supplier can approach 100 percent of the stated cost.

An organization that continually uses pirated or unsupported software will likely develop a culture of avoiding–rather than actively pursuing–interactions with its software's producers. Although some software companies claim to provide software patches to customers even after they stop paying for licenses, in practice those using pirated network software rarely receive updates from the vendors.[34] It is a source of debate as to where the blame lies. On the one hand, users complain of significant technical hurdles for updating unregistered software. On the other hand, vendors claim that few network administrators overseeing unlicensed copies ever seek them out, leaving them unaware of who is running pirated copies of their unpatched software. In either case, the presence of pirated software increases the likelihood that the organization's network is susceptible to vulnerabilities.[35] Even if an unregistered organization seeks out and applies a patch, because the process is not timely or automatic, there will always be a window of time with unpatched vulnerabilities.

In evaluating their country's cybersecurity posture, governments in the Global South must measure the degree to which pirated and unpatched software is present on their information platforms and identify mechanisms that can decrease their rate of use. It may be wise for policymakers to look at culture and practice instead of simply increasing IT budgets. Comparative country research shows that the income of countries or individual enterprises was not a consistent predictor of choosing licensed or pirated software. Instead, the strongest predictors were a tolerance of open pirated software markets and the degree of systemic corruption in the country.[36] Moreover, a comparison of a half dozen policy measures in eleven African countries found that the strongest initiative reducing the presence of pirated soft-

28 Jonathan Klaaren et al., "Public Procurement and Corruption in South Africa," Public Affairs Research Institute, October 2022, https://ideas.repec.org/p/osf/osfxxx/bej9z.html.

29 Rajeev K. Goel and Michael A. Nelson, "Determinants of software piracy: economics, institutions, and technology," *Journal of Technology Transformation* (2009), 34, https://link.springer.com/article/10.1007/s10961-009-9119-1.

30 "Software Management: Security Imperative, Business Opportunity," Business Software Alliance, June 2018, https://www.bsa.org/files/2019-02/2018_BSA_GSS_Report_en_.pdf.

31 Brian Prince, "Software piracy costly to enterprise security, research finds," *Security Week*, March 20, 2014, https://www.securityweek.com/software-piracy-costly-enterprise-security-research-finds/.

32 "Drivers of Corruption: A Brief Review," The World Bank, 2014, https://documents1.worldbank.org/curated/en/808821468180242148/text/Drivers-of-corruption.txt.

33 David P. Nolan, "Procurement fraud – an old fraud flourishing in emerging markets and costing businesses billions," *Financier Worldwide Magazine*, September 2017, https://www.financierworldwide.com/procurement-fraud-an-old-fraud-flourishing-in-emerging-markets-and-costing-businesses-billions#.Y-jdcC-B3X8.

34 Angela Moscaritolo, "Losses from software piracy leads $51 billion in 2009," *SC Media*, May 13, 2010, https://www.scmagazine.com/news/losses-from-software-piracy-exceed-51-billion-in-2009.

35 Atanu Lahiri, "Revisiting the incentive to tolerate illegal distribution of software products," *Decision Support Systems* (2012), vol. 52, no. 2, 2012, https://doi.org/10.1016/j.dss.2012.01.007.

36 Peerayuth Charoensukmongkol et al., "Analyzing software piracy from supply and demand factors: The competing roles of corruption and economic wealth," *International Journal of Technoethics* (2012), vol. 3 no. 1, https://econpapers.repec.org/article/iggjt0000/v_3a3_3ay_3a2012_3ai_3a1_3ap_3a28-42.htmhttps://econpapers.repec.org/article/iggjt0000/v_3a3_3ay_3a2012_3ai_3a1_3ap_3a28-42.htm.

ware on networks was implementing corruption-control policies, not measures that raised incomes or procurement budgets.[37]

Case Study: IT Procurement Corruption in Pakistan

Even donor-funded procurement can fall victim to IT procurement schemes. Drawing on a 2019 World Bank loan, the Pakistan Federal Board of Revenue (FBR) used $80 million to upgrade the Karachi data center as its hardware and software were no longer supported by vendors and had been assessed as "end-of-life equipment."[38] Just a year after the procurement, the US Assistant Secretary of State Alice Wells publicly accused FBR of using pirated versions of US software in the data center.[39] A year later, a suspected Russian cybercriminal gang gained access to the center's more than 1,500 computers and data; reportedly benefiting from the pirated and unsupported Microsoft Hyper-V software used for the virtual hard disks storing FBR data.[40] The FBR has never identified the vendor involved in the World Bank procurement or whether they paid the ransom to unlock their data that was advertised for sale on a Russian dark web site.

As countries struggling with public corruption or high levels of pirated software integrate further into the global digital economy, they are increasingly susceptible to cyberattacks on their critical infrastructure. Some observers already view 2022 as an inflection point in the rising number of successful hacks of smaller countries.[41] In July 2022, for example, the government of Albania was forced to shut down its government computer and internet systems after a devastating cyberattack. The intrusion was a result of an unpatched version of the file-sharing software Microsoft SharePoint Server (versus the more common cloud-based Microsoft 365 SharePoint) that understaffed IT teams had maintained for years on their networks.[42] Albania has not chosen to explain how its software did not get the patch for this vulnerability released automatically by Microsoft two years earlier. As mentioned previously, the island nation of Vanuatu was also hit by a ransomware attack in 2022 that froze nearly all government network servers, shutting down fire and rescue services, erasing five months of court data, and preventing 315,000 citizens from paying taxes or utilities.[43] That same year, two more ransomware attacks by the Russia-based Conti Group led the Costa Rican government to declare a national emergency,[44] and cybercrime groups also temporarily gained control of government networks in Montenegro and Chile.

Regardless of the technical cause, the lessons from these examples are the same: Countries seeking to protect networks across their critical infrastructure must prioritize systematic communications with software developments and implement regular updates or face an army of hackers that target unpatched vulnerabilities to gain control of a network.

The ascendancy of cyberattacks in the Global South buoyed by these successful breaches also suggests that cybercriminals are now targeting small or economically challenged countries because they may be viewed as "softer" hacking targets. Certainly, enterprises around the world continue to pay ransomware, as 2023 set a record for total and average payments of ransoms. The recent cybercriminal focus on the Global South, however, may partly reflect a perception that their networks represent lower-risk targets with a higher willingness to pay for returning access to their data.[45] The strong correlation between systemic corruption and a preference for pirated software may shape an approach to ransomware that is appealing to cyber criminals. If an organization's management has been earning significant kickbacks on purchases of pirated software, for example, they are unlikely to pursue a strategy of resisting ransom requests, instead quietly choosing to pay and maintain the status quo. The focus on the Global South may also reflect a landscape of reduced opportunities in the Global North. Leading ransomware

37 Antonio R. Andres and Simplice A. Asongu, "Fighting software piracy: Which governance tools matter in Africa?" *Journal of Business Ethics* (2013), 118, https://www.econstor.eu/bitstream/10419/87824/1/730896803.pdf.

38 Rana Shahbaz, "Neglect caused FBR cyber-attack," *The Express Tribune*, August 22, 2021, https://tribune.com.pk/story/2316604/neglect-caused-fbr-cyber-attack.

39 Jehangir Nasir, "US accuses FBR of using pirated software," *ProPakistani.* January 30, 2020, https://propakistani.pk/2020/01/30/us-accuses-fbr-of-using-pirated-software-report.

40 Haroon Hayder, "Here's the real reason why FBR system got hacked," *ProPakistani*, August 20, 2021, https://propakistani.pk/2021/08/20/heres-the-real-reason-why-fbrs-system-got-hacked/.

41 Cynthia Brumfield, "2022 was the year of crippling ransomware attacks on small countries," *README Blog*, December 16, 2022, https://readme.security/2022-was-the-year-of-crippling-ransomware-attacks-on-small-countries-e63b5bc3b756.

42 "Microsoft investigates Iranian attacks against the Albanian Government," Microsoft, September 8, 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government.

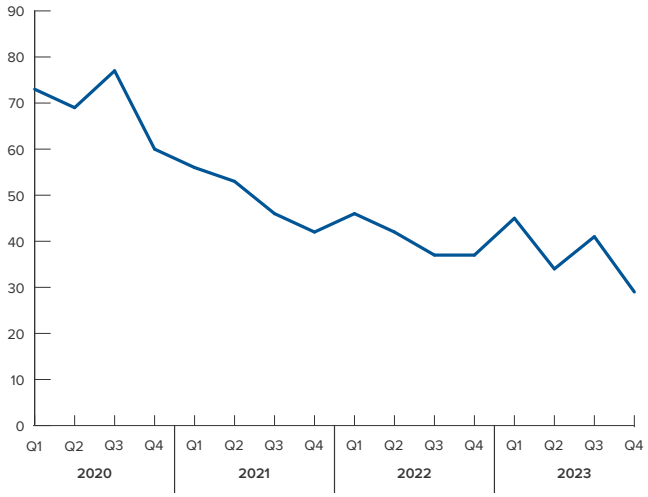
43 Christopher Cottrell, "Vanuatu officials turn to phone books and typewriters, one month after cyberattack," *The Guardian*, November 29, 2022, https://www.theguardian.com/world/2022/nov/29/vanuatu-officials-turn-to-phone-books-and-typewriters-one-month-after-cyber-attack.

44 Matt Burgess, "Conti's attack against Costa Rica sparks a new ransomware era, *Wired*, June 12, 2022, https://www.wired.co.uk/article/costa-rica-ransomware-conti.

45 Andy Greenberg, "Ransomware payments hit a record $1.1 billion in 2023," *Wired*, February 7, 2024, https://www.wired.com/story/ransomware-payments-2023-breaks-record.

negotiator Coveware recently reported that the portion of victims in the U.S. paying the ransom has fallen by half over the last three years (See Figure 3); the same exact period that has seen a dramatic increase in attacks on enterprises in the Global South.[46]

Figure 3: U.S. Paid Ransom (%)



DATA SOURCE: COVEWARE (VIA BLEEPINGCOMPUTER.COM)

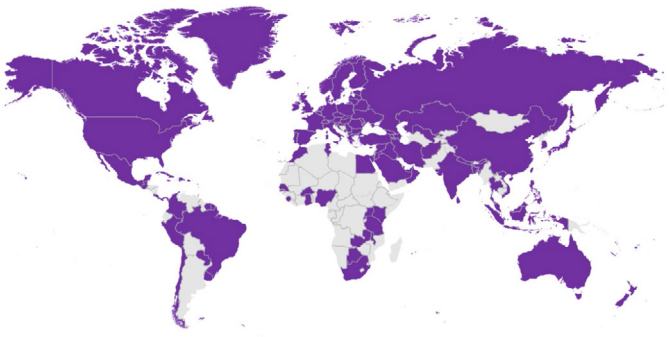
Moving forward, more and more government institutions and critical infrastructure enterprises in the Global South will likely be targeted as they continue to integrate with global information and communication networks. What is less certain is whether the procurement culture in these countries can keep up by transforming from one of avoiding the attention of software developers to a strategy of maximizing communication and exchanges. This transition is unlikely to succeed if corrupt practices continue to incentivize avoiding transparent procurement and collaboration with vendors to support resilient network systems. Moreover, the transition will require a proactive government guided by a clear national cybersecurity strategy that addresses the unique cyber policy challenges in the Global South.

WHAT IS IN THE NATIONAL CYBERSECURITY STRATEGIES – AND WHAT ISN'T

As digital connectivity continues to expand, more than 100 countries have developed national cybersecurity strategies to serve as the framework for synchronized public-private cybersecurity development. A review of the twenty-three published national strategies from countries in Africa and the Asia-Pacific region found that, in general, the strategies' objectives were grouped across a minimum of four pillars for strengthening cyber resilience.[47]

The first common pillar consists of strategic objectives that often include developing new cybersecurity agencies and/or improving coordination between disparate ministries overseeing cybersecurity policy. This pillar also includes new policy initiatives based on gap analyses of the country's cybersecurity architecture. The government's structural reform steps are often intertwined with the second pillar of legislation and regulations. The Council of Europe has been the most influential donor in this space, assisting in the development of legislative frameworks and advising in the development of national cybersecurity strategies in at least nineteen countries in the Global South.

Figure 4: Countries with National Cybersecurity Strategy



SOURCE: INTERNATIONAL TELECOMMUNICATION UNION

The last two pillars focus on external initiatives. The third pillar is focused on public-private partnerships, including cooperation with multinational software producers and other governments pursuing cybersecurity. The fourth major pillar usually describes information campaigns and education initiatives that would strengthen cybersecurity in the workforce. While national strategies in the Global South have prescribed more limited activities in the fourth pillar, the EU has recently joined the US in developing cybersecurity workforce frameworks to bridge the gap between the planning and development of cybersecurity educational standards and the workplace requirements for the knowledge and skills needed to defend critical infrastructure networks.

Across the national cybersecurity strategies in the Global South, not one of the twenty-three documents contained the terms "corruption" or "pirated software." In some ways, this is not surprising. The leading roadmap to developing a national cybersecurity

46 Bill Toulas, "Ransomware payments drop to record low as victims refuse to pay," *Bleeping Computer*, January 29, 2024, https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-as-victims-refuse-to-pay/.

47 The review of 23 national cybersecurity strategies consisted of 14 documents published by countries in Africa (Botswana, Benin, Burkina Faso, Gambia, Ghana, Kenya [draft], Malawi, Mauritius, Mozambique [draft], Nigeria, Sierra Leone, South Africa, Tanzania, and Uganda); and 9 documents published by countries in the Asia-Pacific region (Afghanistan, Bangladesh, China, India, Malaysia, Nepal [draft], Philippines, Samoa, and Vanuatu).

strategy, the UN's International Telecommunication Union's (ITU) Guide to Developing a National Cybersecurity Strategy, also does not reference corruption or pirated software. The 2018 guide was produced by a partnership between ITU, the World Bank, the Council of Europe, the Organization of American States (OAS), Interpol, Microsoft, Deloitte, and the NATO Cooperative Cyber Defense Center of Excellence, as well as several think tanks. The guide specifically states its objective is "to "provide direction and good practice on 'what' should be included in a National Cybersecurity Strategy, as well as on 'how' to build, implement and review it."

Case Study: International Counter Ransomware Initiative

The most significant US-sponsored global cybersecurity initiative is arguably the International Counter Ransomware Initiative (CRI). Now in its third year of existence, the group has established a platform for capacity building and developing best practices to reduce the success of ransomware, including via a joint statement that member countries should not pay ransoms.[48] Although more than a dozen of the fifty nation-state participants in the CRI are considered Global South countries that face significant challenges in addressing systemic corruption, the CRI's policy and capacity-building efforts have so far followed the ITU and World Bank's lead in not addressing procurement corruption as part of cybersecurity initiatives.[49]

As representatives of government and civil society in the Global South look to further develop and reassess their national policies and infrastructure for cybersecurity, they are unlikely to find anti-corruption best practices in the prevailing guiding documents and best practices. The reality is that top cybersecurity officials in North America and the EU do not consider the role of corruption to be a major or even minor factor in their country's cybersecurity resilience. Instead, countries in the Global South must consider the context of corruption and its impact on cybersecurity and critical infrastructure resilience when developing their strategies, as well as learn from the experiences of other states' adoption of reform initiatives focused on procurement corruption.

GLOBAL SOUTH LESSONS LEARNED: THE UKRAINIAN RESPONSE TO CORRUPTION

Ukraine offers a case study of how a country challenged by systemic corruption can reduce its impact on network security. In the years leading up to the start of open conflict with Russia in 2014, on more than one occasion senior officials in Ukrainian ministries iterated to the author that they would rather cancel a project than not receive their preference for an expensive network software solution. In at least one case this prevented a donor-supported project from moving ahead as the ministry refused to use a simpler, less expensive software product that was more aligned with their needs and local network. Across several ministries, the practice of procuring the highest-cost network solutions over this period would result in arrears owed to the vendor due to the inability to pay annual fees. At one point, the sales representative of a global network software company told the author that they would not sell new software to a US-funded project if the ministry did not agree to pay off years of outstanding annual license fees owed from past procurement.

By late 2014, as the first wave of cyberattacks on Ukraine preceded the Russian military's annexation of Crimea, most critical state infrastructure had been operating for years without licenses (and the associated updates and patches), even legally purchased software.[50] Many institutions were instead paying a fraction of the retail price to obtain pirated versions of software, which conveniently left the bulk of the recorded procurement expenditures for corrupt rent-seeking. This explains how, prior to 2014, an estimated eighty percent of the network software used in Ukrainian private and public enterprises either never had been or no longer was supported by the software's vendors.[51]

As hackers associated with Russia began cyberattacks in support of the new "special operation" in Ukraine, they targeted local software commonly used in the two countries by exploiting vulnerabilities for which patches had not been installed.[52] Most notably, in 2015 the Russian military hacker group Sandworm used Blackenergy-3 malware to temporarily knock out the information networks of three energy distribution companies, denying power to more than 200,000 homes in 2015. The next year, the Industroyer-1 malware was used to target the Kyiv region's

48 Michael Hill, "Governments should not pay ransoms, International Counter Ransomware initiative members agree," *CSO*, November 2, 2023, https://www.csoonline.com/article/657877/governments-should-not-pay-ransoms-international-counter-ransomware-initiative-members-agree.html.

49 "International Counter Ransomware Initiative Joint Statement," The White House, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement.

50 Olena Removska and Robert Coalson, "Ukraine's trade privileges on line over intellectual piracy concerns," Radio Free/Radio Liberty, March 14, 2013, https://www.rferl.org/a/ukraine-sanctions-intellectual-property/24928537.html.

51 "Software management: Security Imperative, Business Opportunity," Business Software Alliance.

52 Patrick Tucker, "Russia launched cyberattacks against Ukraine before ship seizures," *Defense One*, December 7, 2018, https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/

power grid.[53] Slovakian cybersecurity firm ESET found that the hackers benefited from knowledge of common post-Soviet electric grid networks and control system software. ESET reported that a major factor in the success of the power grid attacks was the failure of Ukrainian electrical distribution enterprises to change obsolete and unpatched operating system software.[54]

In arguably the most damaging cyberattack in history, in 2017 the Sandworm group unleashed the NotPetya wiper malware that specifically targeted a well-publicized vulnerability in Microsoft network software that the company had patched in updates a few months before the attack. At that time, most Ukrainian enterprises were using either pirated or older versions of Microsoft data management software and thus did not receive timely or automatic updates.[55] Although Microsoft and other vendors in principle permit operators of pirated software to request and apply updates, this is rarely accomplished and the exploitation of unprotected networks in Ukraine accounted for more than an estimated $10 billion in commercial losses.[56] The NotPetya malware is also an example of a software vendor advertising new software updates after an attack. A secondary effect of this disclosure, however, is that it provides hackers a roadmap for similar attacks on other unpatched systems in the Global South.

POLICY RECOMMENDATIONS DRAWN FROM UKRAINE

Since 2017, Ukraine has adopted, with mixed results, a range of internal and donor-supported anti-corruption initiatives ranging from the establishment of investigation bureaus to prosecuting state corruption and mounting ad campaigns that promote good governance.[57] One of the most well-known developments, which also had an outsized impact on software procurement corruption, is the launch of a national e-government tool for public procurement.[58] A public/private-administered electronic platform for government tenders, ProZorro, which means "through transparency" in Ukrainian, began operating with more than 300 private suppliers in 2016. ProZorro largely put an end to backroom procurement processes in Ukraine by making bidding and decision-making available to the public, which reduces opportunities for rent-seeking.[59]

Over the next four years, additional legislative and operational improvements were made to ProZorro, including integrating the role of tax authorities directly onto the platform to provide additional oversight for fraudulent pricing and hidden kickback schemes. By gaining private sector support early in its development, ProZorro was able to move the government's IT infrastructure purchases onto a platform by 2019, which by then was facilitating $22 billion worth of tenders across the government.[60] In a sign of trust in the transparency and efficiency of ProZorro, the World Bank has also began conducting its own Ukrainian procurement through the platform.[61]

In 2022, the Computer Emergency Response Team of Ukraine (CERT) reported a total of 2,194 investigated malware attacks, twenty-five percent of which targeted government systems, with at least a dozen cases in which the malware was detected on critical infrastructure information systems.[62] Nonetheless, the work of the CERT, bolstered by robust private sector partnerships with software developers, led to quick responses to patch identified vulnerabilities before malware could spread and result in significant network outages. The result of this new capacity has been the prevention of cyber-induced infrastructure outages such as the electric grid collapses that plagued Ukraine in 2015-2016.[63]

In the years following the NotPetya attack, Ukrainian public and private organizations began addressing old debts to network

53 Mark Temnycky, "Russian Cyber Threat: US Can Learn from Ukraine," *Atlantic Council*, May 27, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/russian-cyber-threat-us-can-learn-from-ukraine.

54 Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet," *We Live Security*, June 12, 2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet.

55 Olena Removska and Robert Coalson, "Ukraine's trade privileges on line over intellectual piracy concerns."

56 Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

57 "Anti-Corruption Reforms in Ukraine: Pilot 5th Round of Monitoring Under the OECD Istanbul Anti-Corruption Action Plan," OECD, 2022. https://www.oecd-ilibrary.org/docserver/b1901b8c-en.pdf?expires=1707274542&id=id&accname=guest&checksum=E8B9D84D2CAB41F47CCF08E6A475AB17.

58 Christopher Yukins and Steven Kelman, "Overcoming corruption and war: Lessons from Ukraine's ProZorro procurement system," *NCMA Contract Management Magazine*, July 2022, https://www.hks.harvard.edu/publications/overcoming-corruption-and-war-lessons-ukraines-prozorro-procurement-system.

59 Andre Petheram, Walter Pasquarelli, and Richard Stirling, "The next generation of anti-corruption tools: Big data, open data, and artificial intelligence," *Oxford Insights*, 2022, https://ec.europa.eu/futurium/en/system/files/ged/researchreport2019_thenextgenerationofanti-corruptiontools_bigdataopendataartificialintelligence.pdf.

60 "Guidelines for non-Ukrainian suppliers on participation in public procurement tenders in Ukrainian," European Bank for Reconstruction and Development, November 2020, https://infobox.prozorro.org/upload/files/main/1398/547/gpa-guide-ukraine-fin-update2020-2.pdf.

61 Nataliya Synyutka, Oksana Kurylo, and Mariya Bondarchuk, "Digitalization of public procurement: The case study of Ukraine," *Annales Oeconomia* (2019), https://journals.umcs.pl/h/article/viewFile/9273/6961.

62 "In 2022, CERT-UA reports 2,194 cyberattacks," *Ukraine Media Center*, January 17, 2023, https://mediacenter.org.ua/in-2022-cert-ua-reports-2-194-cyberattacks-a-quarter-of-them-against-government-agencies-state-service-for-special-communications/

63 Jon Bateman, "Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications," *Carnegie Endowment for International Peace*, 2022, https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_Cyber-FINAL21.pdf.

software vendors while using the ProZorro platform for new IT procurement. As a result, the country's state-owned critical infrastructure operators were forced to pursue open tenders on a public-private run platform while network software companies returned to selling licenses to the state enterprises. The author was told by senior officials at Ukraine's State Special Communications Service (SSCS) that they estimated the share of pirated and unsupported software on the country's networks had dropped from more than eighty percent at the start of the conflict with Russia in 2014 to only twenty percent in 2020

While state enterprises have been required to make transparent software purchases since 2020, anti-corruption progress in the private sector is less certain. As part of the 2022 Russian cyberattacks on Ukraine, the Mandiant cybersecurity firm found that Russian military intelligence hackers likely uploaded "trojanized" versions of Microsoft software on torrent sites popular with Ukrainians.[64] The malware was part of the Ukrainian language packs that, if selected, would perform reconnaissance on a system and install further malware as needed.

The commitment of state critical infrastructure in Ukraine to rapidly expand licensed software on their networks also drew the interest of large international software vendors that saw Ukraine as ground zero in identifying new malware.[65] Therefore, as Ukrainian public and private sector enterprises pursued legitimate purchases of licensed software, they also found that vendors were just as motivated to repair relationships with Ukraine's large network operators. A benefit that few could have predicted in 2016 at the start of Ukraine's anticorruption agenda is the role that the return of licensed software vendors would have in countering the much larger volume of cyberattacks that accompanied the 2022 Russian invasion. The major network software vendors, such as Microsoft and Cisco, established computer response and threat intelligence teams in Ukraine as part of their effort to identify and mitigate new threats to their licensed software before the malware targeting Ukraine could become a global problem.[66]

The transformation of Ukrainian cybersecurity resilience over the five years between the last of the most harmful cyberattacks on the country (WannaCry and NotPetya) in 2017 and the resilience in the face of the relentless wave of malware attacks that accompanied Russia's 2022 full-scale invasion suggests governments can proactively make progress against serious systemic vulnerabilities. Nonetheless, the anti-corruption approach must be relentless to succeed. For example, it was no surprise when in late 2023 national anti-corruption investigators uncovered a large IT software kickback where two senior SSCS officials had falsely categorized some procurement as classified, keeping it from being posted on the ProZorro site.[67]

Overall, the Ukrainian experience suggests that countries burdened with systemic corruption should integrate procurement reform into their cybersecurity measures to mitigate the impact of cultures across the Global South that have promoted or looked the other way at the use of pirated or unsupported software.

ADDRESSING CORRUPTION IN CYBERSECURITY STRATEGIES

The decision by a dozen of the world's most influential institutions promoting international cybersecurity not to address the threat of systemic corruption in their 2018 Guide to Developing a National Cybersecurity Strategy continues to be echoed in advisory and technical assistance offered to countries in the Global South. A recent example is the removal of considerations for sectoral vulnerability to procurement corruption in the World Bank's 2023 influential sectoral cyber capability maturity model (C2M2) assessment tool, which was originally present in the pioneering PRoGReSS sectoral C2M2 developed by Tel Aviv University that the assessment tool is based upon.[68]

It is clear from the Ukrainian case study that neglecting issues of corruption in software procurement may result in overlooking an important lever for reducing overall cyber vulnerabilities. While officials in both the Global South and Global North tend to avoid public discussions of corruption, Ukraine's IT procurement transparency reform offers cybersecurity policymakers a more targeted and politically acceptable policy goal. Certainly, the absence of guidance on IT procurement corruption is leaving cybersecurity strategists in countries challenged by systemic corruption without inspirational goals or advice on mitigating a key threat to their critical infrastructure networks.

As profiled in this analysis, Pakistan offers a cogent example of a country seeking to address its vulnerability to IT procurement corruption. Just two years after a Russian ransomware organization gained complete access to the revenue service's new data center riddled with unsupported software, the Ministry of

64 "Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government," Mandiant Intelligence, "December 15, 2022, https://cloud.google.com/blog/topics/threat-intelligence/trojanized-windows-installers-ukrainian-government/.

65 Emma Schroeder and Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment," *Atlantic Council*, February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment.

66 Robert Peacock, "How Ukraine has defended itself against cyberattack – Lessons for the US," *The Conversation*, April 5, 2022, https://theconversation.com/how-ukraine-has-defended-itself-against-cyberattacks-lessons-for-the-us-180085.

67 Daryna Antoniuk, "Second top Ukrainian cyber official arrested amid corruption probe," *The Record*, November 27, 2023, https://therecord.media/second-cyber-official-detained-zhora.

68 "Sectoral Cybersecurity Maturity Model," The World Bank, June 2023, https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P17263707c36b702309f7303dbb7266e1cf.pdf.

Foreign Affairs official responsible for cybersecurity championed the need to adopt national policies in line with the 2018 Guide to Developing a National Cybersecurity.[69] The Guide offers a robust set of recommendations and certainly should influence Pakistan's implementation of its 2021 national cybersecurity strategy, but a government that witnessed first-hand how procurement corruption undermines critical infrastructure cybersecurity would also have benefited from the inclusion of guidance and materials on targeted procurement anticorruption measures—advice not found in the 2018 Guide.

The dramatic turnaround in the resilience of Ukrainian networks demonstrates the importance of cybersecurity strategies that include the adoption of external and transparent procurement platforms for critical infrastructure enterprise software and technology. As with any capacity-building measure, a cybersecurity anti-corruption initiative could start small as countries struggle to wrestle public procurement from rent-seeking interest groups. A national public tender system that covers all procurement, such as Ukraine's ProZorro, is an ambitious goal that requires years to develop and operationalize. Nevertheless, national cybersecurity strategies could promote more limited platforms focused on critical infrastructure enterprise procurement from the handful of network software providers serving the market.

IT procurement reform success depends on the degree to which sectoral or national institutions introduce public-private collaboration, transparency, and autonomy into decision-making processes that currently happen in the backrooms of state bureaucracies. A failed approach was demonstrated in Kenya when the centralization of IT procurement within a single ministry led to the doubling or tripling of prices for key technologies negotiated by newly empowered senior officials.[70] Kenya's cybersecurity strategists should be credited with seeking to address the vulnerabilities linked to IT procurement processes. Moreover, they were proposing solutions in a sphere (IT procurement reform) that international donors and cybersecurity consultants continue to avoid.

The most durable solution is for national cybersecurity strategies to begin to address procurement processes to remove the role of illicit rent-seekers in transactions. Kenya's failed 2019 centralization of state IT procurement is an example of how many countries in the Global South have only adopted narrow measures limiting the impact of reform to just IT procurement. The next step would be to further limit that procurement to transparent and external electronic tender platforms modeled on Ukraine's ProZorro system. The e-tender process would serve to transform the country's critical infrastructure networks by shifting procurement to licensed and updated network software while attracting increased software vendor competition because sales revenues are no longer flowing back to rent-seeking IT administrators.

A shift in national cybersecurity strategies toward the adoption of e-tender platforms can be facilitated by the rapid growth in e-governance across the Global South. The first generation of e-tender platforms, like ProZorro, were "semi-distributed" to the degree that public and private entities supervise their analytical dashboards across the platform.[71] The growing role of blockchain technology in creating transparent contracts across peer-to-peer networks will certainly transform the next generation of transparent procurement platforms.

Addressing IT procurement vulnerabilities can also build on existing resilience measures in national cybersecurity strategies. For example, cybersecurity awareness campaigns championed in existing national strategies can be leveraged to have a potential anti-corruption role. Their messaging could target not only individuals but also enterprises while highlighting the vulnerabilities that follow the choice to adopt pirated or other unsupported software. A generation of IT managers, who spent decades downloading pirated software for their personal use, must understand that those practices are no longer safe in the era of the ransomware gang and their recent turn toward targeting the Global South.

Another strategy that often is proposed as a cybersecurity solution for budget-constrained institutions in the Global South is open-source software (OSS). Paying for commercial software is not the only means to reduce the portion of pirated software on an enterprise's network. OSS software has long been the building blocks of the world's dominant network software sold by private vendors, and for more than two decades governments in the Global North have been adopting requirements mandating that officials first seek OSS alternatives before purchasing commercial software for their critical infrastructure networks.[72] Nonetheless, malware has increasingly been targeting open-source solutions and a policy shift toward OSS in the Global South must be part of a wider government-led effort to recognize the need to support OSS as another element of critical infrastructure.[73]

69 Shahrukh Khan, "Cybersecurity Challenges in Pakistan: An Assessment," *Science Diplomacy*, March 2022, https://www.researchgate.net/publication/360256123_Cyber_Security_Challenges_in_Pakistan_An_Assessment.

70 Wanjohi Githae, "Concern over graft as state centralizes IT procurement," *Nation*. January 12, 2019, https://nation.africa/kenya/news/concern-over-graft-as-state-centralises-it-procurement--127312.

71 Pedro Bustamante, et al., "Government by code? Blockchain applications to public sector governance," *Frontiers in Blockchain* (2022), vol. 5, https://doi.org/10.3389/fbloc.2022.869665.

72 Benjamin J. Birkinbine, *Incorporating the Digital Commons: Corporate Involvement in Free and Open Source Software*, (London: University of Westminster Press, 2020), https://library.oapen.org/bitstream/handle/20.500.12657/37226/1/incorporating-the-digital-commons.pdf.

73 Stewart Scott, et al., "Avoiding the success trap: Toward policy for open-source software as infrastructure," *Atlantic Council*, August 8, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/open-source-software-as-infrastructure/.

As countries continue to innovate in measures to raise transparency in the procurement of IT software and hardware, donors should reconsider their past hesitancy to advocate for anti-corruption measures as part of the cybersecurity strategies they support. The absence of even indirect references to the role of corruption in national cybersecurity strategies across the Global South is inexplicable given the serious cybersecurity risks that are present for countries standing up large information networks founded on pirated or unsupported software. Given the significant challenges developing countries face in responding to cyber threats, they cannot afford to simultaneously overlook the vulnerability associated with corrupt procurement practices.

CONCLUSION

Developing countries are continuing to make progress in digitizing governance and trade while simultaneously raising transparency in their public expenditures. Nevertheless, 2022's country-wide network outages across the Global South suggest this capacity has been built on networks left vulnerable by unlicensed and unsupported software. As governments and critical infrastructure in the Global South prepare for the next stage in ICT development, they must prioritize policies that can reduce corruption in the critical procurement of the network software responsible for protecting their country's nascent cyberspace. As Adam and Fazekos argue, reform-minded governments and donors throughout the Global South have adopted ICT practices in the fight against national corruption but have developed a blind spot to the role corruption plays in undermining the security of this rapid digitization.[74]

Cybersecurity strategists working in the Global South must reevaluate a decade of national strategies that largely replicated those from the Global North. It is no longer safe to assume that cyber best practices are divorced from the harsh reality of addressing systemic corruption. At a minimum, national cybersecurity strategies must, for the first time, identify procurement corruption as a cybersecurity risk. Moreover, countries challenged by systemic corruption and under-resourced governance should consider more limited initiatives, such as creating transparent and autonomous IT tender processes for the most critical state sectors. The digital integration of the Global South offers its citizens greater prosperity and transparency in governance, but as decades of past economic development have demonstrated, the equity and reliability of this new revenue stream will depend on leaders not overlooking the adverse impact corruption can play in the social outcomes of their digital development.

ABOUT THE AUTHOR

Robert Peacock is a nonresident senior fellow at the Cyber Statecraft Initiative of the Atlantic Council's Digital Forensic Research Lab, where his work builds on his past role supporting the highly correlated goals of reducing corruption in critical infrastructure procurement and developing cybersecurity resilience in the Global South. Peacock currently is Senior Strategic Technical Advisor at DAI Global advising on cybersecurity development programs, funded by the US Agency for International Development (USAID), across a half dozen countries in Eastern Europe and Eurasia. Peacock's past advisory roles have included developing assistance programs in Armenia, Mozambique, Morocco, while more recently serving as a co-creator for USAID's first bilateral cybersecurity program (Ukraine) and first regional cyber pathway for women program (Balkans).

74 Isabelle Adam and Mihaly Fazekas, "Are emerging technologies helping win the fight against corruption? A review of the state of the evidence," *Information Economics and Policy* (2021), vol. 57, December 2021, https://www.sciencedirect.com/science/article/pii/S016762452100038X.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
Dario Deste
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of April 24, 2024

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org