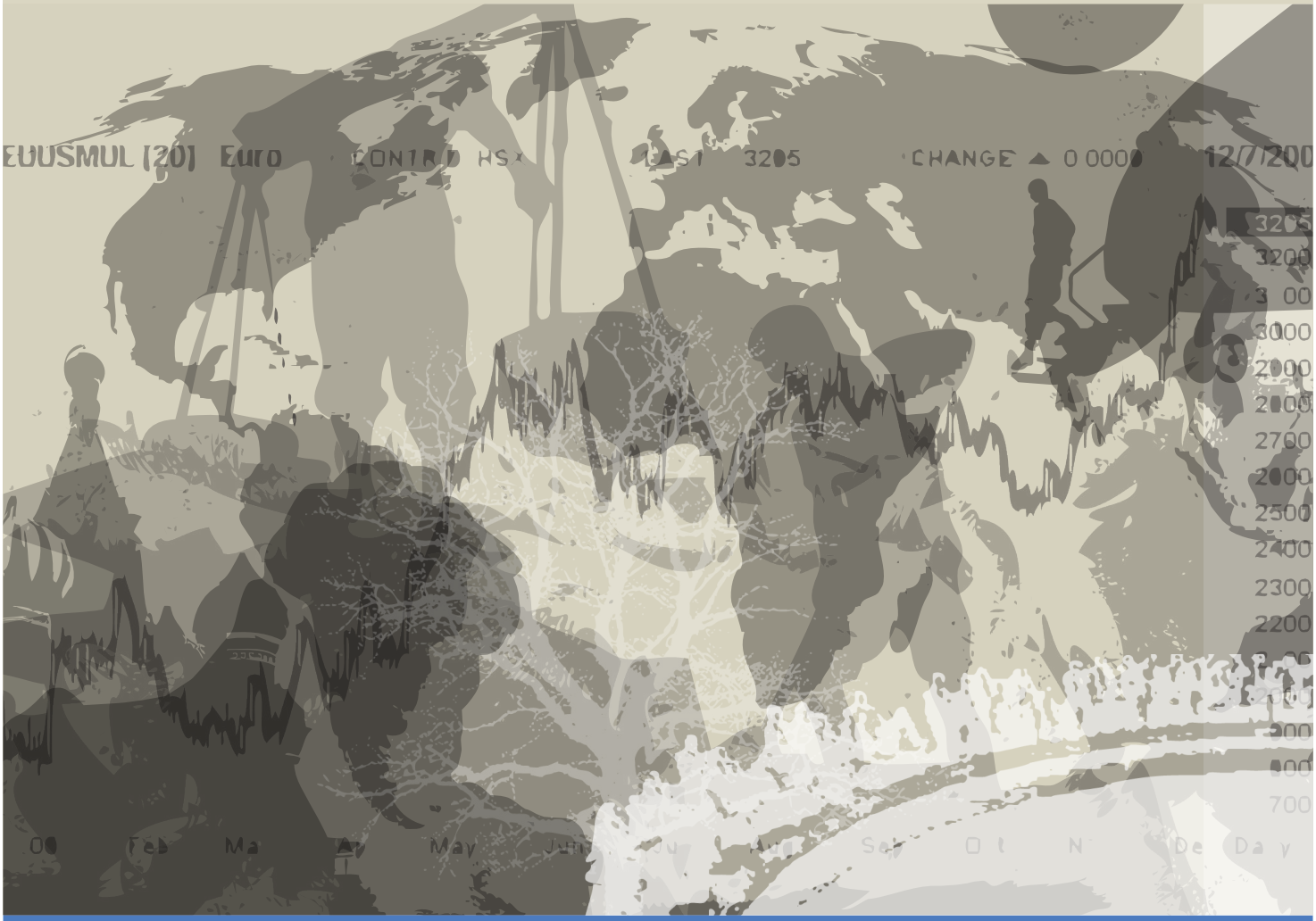
Norwegian Institute of International Affairs

Cyber Security Capacity Building: Security and Freedom

Hans-Inge Langø



NUPI Report
[Report no. 1, 2016]

Publisher: Norwegian Institute of International Affairs

ISBN: 978-82-7002-337-0

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: post@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

Cyber Security Capacity Building: Security and Freedom

Hans-Inge Langø

Published by the Norwegian Institute of International Affairs

Contents

Introduction

In the past decade, access to information communication technology (ICT) has surged across the world. Broadband technology is now available to billions more than it was just years ago. The growth has been particularly strong in mobile-based subscriptions; by 2014 in the developed world there were 84 active mobile broadband subscriptions per 100 inhabitants. Although there were only 21 in 100 subscriptions in the developing world in the same period, the fastest growth has been in Africa, rising from 2 percent penetration in 2010 to almost 20 percent by 2014. Add to this a slower but still positive growth in fixed broadband subscriptions, and we see that the world is becoming increasingly wired for Internet access.[1]

The diffusion of ICT comes with several economic benefits. Electronic commerce (e-commerce) can improve efficiency and productivity—but there are significant barriers to reaping these and other benefits, particularly in developing countries. The challenges include poor telecommunications infrastructure, transactional trust, and payment systems.[2] While there is much variation in capacity across the world, Africa is consistently mentioned as the weakest region. According to the International Telecommunications Union, Africa ranks lowest on their ICT Development Index, and only two countries in the region score above the global average (Mauritius and Seychelles).[3] Another survey of network readiness shows that the state of ICT infrastructure is particularly poor in sub-Saharan Africa, despite the increase in cellphone and Internet users.[4] Not all these issues can be solved solely by building cyber-capacity—but at a minimum the new e-commerce should be stable and safe, in order to ensure the consumer and business trust essential for continued growth.

---

1 International Telecommunications Union, *The World in 2014: ICT Facts and Figures.* (Geneva: International Telecommunications Union, 2014).

2 Japhet Eke Lawrence and Usman A. Tar, "Barriers to E-Commerce in Developing Countries," *Information, Society and Justice Journal* 3, no. 1 (2010): 23–35.

3 International Telecommunications Union, *Measuring the Information Society Report 2014* (Geneva: International Telecommunications Union, 2014).

4 Benat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, "The Global Information Technology Report 2014" (Geneva: World Economic Forum, 2014).

The threats associated with ICT are multifaceted. The present report posits that cyber-capacity building (CCB) should not be considered simply a risk-management endeavor. The potential for malware, cyber-attacks, and cyber-crime are not the only challenges associated with the rapid spread of ICT. Policymakers must also consider the intersection of technology and politics, particularly in developing countries still transitioning into democracies.

They must do so because ICT can be used to overcome collective action problems. Under the right circumstances, this process may mean democratization, as the technology can enable more information and better coordination between people. In other contexts, however, the same technology may enable or accelerate violent rebellion. Governments can choose from a wide range of policies for confronting either situation, but the most harmful would be the application of repressive techniques in order to combat peaceful opposition. ICT can potentially be either a boon or a threat to democracy; it can aid peaceful opposition or violent rebellion; help governments enforce the rule of law or repress the population. Formulating a policy for building cyber-security capacity must take these threats and risks into account.

Threats, risks and challenges

This report builds on the assumption that the primary goal of building cyber-capacity is to reduce the risk and cost of malicious activity in and through cyberspace as incurred by developing countries. This requires building institutional capacity within these countries in order to prevent, detect, and handle cyber-incidents. Such incidents generally involve the use of malware to gain unlawful access to networks in order to steal information or sabotage processes. Actors may steal sensitive information for financial gain, or attack critical national infrastructure (e.g. telecommunications infrastructure, power grids, or financial markets) to cause widespread disruption.

These various types of cyber-attacks can cause significant damage, as seen in developed countries over the past decade. Estimates differ wildly, but the direct costs of cyber-crime are estimated at billions of dollars each year.[5] Furthermore, the theft of proprietary information and technology, such as military secrets, can have long-term financial and strategic costs that are difficult to estimate. It is reasonable to assume that also developing countries incur these costs, although the lower level of ICT penetration might mean they are less dependent and thus less vulnerable to cyber-attacks, resulting in lower costs. Furthermore, people in developing countries rely largely on wireless Internet access, and cellphone malware is far less developed or widespread than malware on laptop and desktop computers.

While the direct costs of cyber-attacks might be seen as the cost of doing business, persistent problems associated with ICT could prove more pernicious. As Thomas Rid as has argued, cyber insecurity can undermine trust between the government and the people.[6] If the government fails to prevent cyber-attacks, the public might see it as ineffectual, or even non-legitimate. This problem could become particularly relevant as the public becomes increasingly dependent on ICT-based services and

5 For some examples of cost estimates, see: Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," *Forbes*, January 17, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/.

6 Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013).

products. Similarly, the public may lose trust in commerce, if Internet fraud and hacking of personal information become commonplace.

Political opposition and rebellion

The diffusion of ICT in a society may have various effects on the population, but arguably the most important is that the technology helps overcome problems of collective action and coordination. Through access to cellphone networks or social media networks, individuals can more easily coordinate, mobilize, and form groups. On the positive side, this democratization of technology may foster democratization itself, as people become empowered by access to more information and to others with similar interests.[7]

Recent years have provided numerous examples of what this process looks like in practice. The Arab Spring, starting in December 2010, showed how social media could undermine authoritarian regimes. While the results have been decidedly mixed for the various opposition movements, Marc Lynch describes various ways in which "the new media" (i.e. television and Internet-based social media) have challenged the power of the Arab states.[8] As expected, these technologies have promoted collective action in various ways. They have lowered the transaction costs for communications and organization, while also creating information cascades. Furthermore, TV and social media have affected international support for the regimes and lessened government control over the public sphere. (Lynch also identifies ways ICT has increased government repression, as discussed below.) In sum, the characteristics of these movements are similar to those of the technology: highly scalable and easily spread, but possibly flat and lacking robust institutional foundations.[9]

---

7 For a broad review of the literature on this topic and the various mechanisms for overcoming collective action problems by the use of ICT, see R. Kelly Garrett, "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs," *Information, Communication & Society* 9, no. 02 (2006): 202–24.

8 Marc Lynch, "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State," *Perspectives on Politics* 9, no. 02 (2011): 301–10.

9 As Lynch notes, "The leaderless, network structures which can hold together a disparate coalition of millions of protestors around a single, simple demand—'Mubarak must go'—are typically far less effective at articulating specific, nuanced demands in the negotiation process which follows success. The Internet may prove to be poor at building warm social networks and trust that are the heart of civil society." Ibid.: 305.

The benefits of ICT for democratization are not universal, however. An empirical study[10] of protest frequency in 22 countries capable of Internet censorship and filtering found no relationship between increased access to the Internet and levels of protests. Increased cellphone access was associated with levels of protest, but yielded different effects depending on the specific circumstances. Countries with already-low levels of protest saw a decrease in protests when cellphone access went up, while countries with high levels of cellphone access saw an increase in protests when cellphone access increased further. These contradictory findings indicate that the introduction of ICT by itself has an indeterminate effect on protests, and any outcome will depend on pre-existing political and economic circumstances.

Despite some promising features, the diffusion of ICT is not without risks. The effects might be highly contingent on a country's political circumstances, since peaceful protesters are not the only ones to have problems in mounting collective action. Rebels and other militant groups can leverage ICT to coordinate violent attacks or even set off cellphone-controlled improvised explosive devices. A recent study of political violence in Africa found that the availability of cellphone coverage increases the probability of violent conflict.[11] While cellphone coverage and conflict levels vary greatly across the African continent, the findings were robust, and indicate that cellphones help overcome collective action problems for rebels and militant groups. However, it is unclear whether these results are generalizable. A study of Iraq during the height of its civil war (2004–2009) found that cellphone coverage decreased insurgent violence. [12] The likely explanation, according to the authors, is that cellphones allowed non-combatant civilians to report insurgent activity to the Iraqi government, thereby aiding their counterinsurgency efforts. The results of these two studies are not necessarily mutually exclusive. As the authors of the Africa study note, referring directly to the Iraq study:

---

10 Patrick Philippe Meier, "The Impact of the Information Revolution on Protest Frequency in Repressive Contexts" (50th International Studies Association Conference, New York, 2009), 15–17.

11 Jan H. Pierskalla and Florian M. Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," *American Political Science Review* 107, no. 02 (2013): 207–24.

12 Jacob N. Shapiro and Nils B. Weidmann, "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq," *International Organization* 69, no. 02 (2015): 247–74.

> We believe it is reasonable that the effects of cell phones are different across these cases. The context of political violence in African countries is much different from that in Iraq. The military capacity of the anti-insurgent forces is likely higher in the case of the U.S. military and government forces in Iraq. While government forces in Iraq have the ability to monitor cell phone activity of insurgents, this is much less likely for many African governments, especially with the more prominent role of private enterprises in spreading technology.[13]

Thus, the effects of cellphone coverage can go either way, depending on the circumstances. One key mechanism here could be the ability of the rebels to impose costs on civilians who help the government. Furthermore, the kinds of capabilities and tactics used by the opposing parties could affect levels of violence. Governments with signals-intelligence capabilities and advanced military capabilities could exploit cellphone coverage to reduce violence, whereas rebels reliant on improvised explosive device attacks could cause violence to increase as cell phone coverage improves.[14]

Repression and surveilance

As the above studies make clear, governments can also leverage ICT to their advantage. A significant risk here is that when faced with opposition, be it violent or nonviolent, a government may opt to repress parts of its population. The literature on state repression is sizeable, and rife with disagreement, but a core finding is what Christian Davenport calls the "Law of Coercive Responsiveness."[15] Briefly put: "When challenges to the status quo take place, authorities generally employ some form of repressive action to counter or eliminate the behavioral threat."[16] The

---

13 Pierskalla and Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," 221.

14 Jacob N. Shapiro and David A. Siegel, "Coordination and Security How Mobile Communications Affect Insurgency," *Journal of Peace Research*, 2015, 0022343314559624.

15 Christian Davenport, "State Repression and Political Order," *Annual Review of Political Science* 10 (2007): 7.

16 Ibid.

successfulness of the repression varies greatly, but the literature indicates that there is more repression in the countries that are not fully democratic or fully authoritarian (referred to as "murder in the middle").[17]

In talking about repression, we are generally referring to overt repressive actions, such as mass arrests. However, more relevant for the discussion here are *covert* repressive actions. These include electronic and physical surveillance—and, unlike overt repression, they are meant to remain hidden, even from the specific target. They are targeted at individuals or groups in order to acquire information about specific or perceived threats to the state.[18] It is this type of government repression that could benefit most directly from the diffusion of ICT; however, such techniques have also been employed on much larger scales.

There is a growing body of literature on the intersection of government repression and ICT. These new technologies have helped some regimes regain control in the face of democratization trends, in some cases even co-opting democratic institutions and processes.[19] In fact, one study found that authoritarian states planning to repress or prevent an independent public sphere were more likely to adopt and expand the Internet than were other autocracies. [20] In this context, governments promote ICT because they see it as a tool of repression. That study found no support for the claim that ICT diffusion led to democratization of the states analyzed.

A groundbreaking study of Chinese censorship of the Internet[21] has given further support to the view of ICT as a tool for overcoming collective action problems. The researchers found that the Chinese authorities

---

17 Helen Fein, "More Murder in the Middle: Life-Integrity Violations and Democracy in the World, 1987," *Human Rights Quarterly* 17 (1995): 170; Patrick M. Regan and Errol A. Henderson, "Democracy, Threats and Political Repression in Developing Countries: Are Democracies Internally Less Violent?," *Third World Quarterly* 23, no. 1 (2002): 119–36.

18 Christian Davenport, "Understanding Covert Repressive Action The Case of the US Government against the Republic of New Africa," *Journal of Conflict Resolution* 49, no. 1 (2005): 120–40.

19 Regine Spector and Andrej Krickovic, "Authoritarianism 2.0: Non-Democratic Regimes Are Upgrading and Integrating Globally" (49th International Studies Association Conference, San Francisco, 2008).

20 Espen Geelmuyden Rød and Nils B. Weidmann, "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes," *Journal of Peace Research* 52, no. 3 (2015): 338–51.

21 Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 02 (2013): 326–43.

were more likely to censure social network posts aimed at coordinating and mobilizing support, than posts criticizing policies or the government.

Governments can also use more blunt tools to prevent mobilization. There have been several instances of authoritarian regimes using network and media disruptions to stifle protest, but the effects have been varied. During the Tahrir Square protests in Egypt in 2010, the regime of President Hosni Mubarak shut down Internet and cellphone access across the country. This blackout actually increased mobilization, however. Navid Hassanpour argues that this happened because full connectivity is in fact bad for mobilization: with insufficient information about the events that were transpiring, Egyptians chose to take to the streets in order to become more informed.[22]

However, under certain circumstances, network and media disruption may have tactical advantages for the regime. In Syria the government has used blackouts to disrupt dissident coordination in conjunction with military operations—but done too often, that may prove counterproductive for the regime, as it can serve as an early-warning system to the opposition. Such disruption is likely to be most successful when used infrequently and temporarily.[23] A related study of government-conducted violence in Syria[24] provides further support to this argument. Distinguishing between targeted and untargeted killings, the study found that higher levels of Internet connectivity were associated with higher levels of targeted killings. These findings indicate that ICT enables better intelligence collection, thus making it easier for the government to target specific threats.

The specific make-up of ICT coverage in a given country has an impact on surveillance and repression. Wireless broadband access far exceeds fixed broadband access in many developing countries, particularly in Africa. As regards collecting data, it should not matter on the technical level whether the population is using mobile phones or desktop computers. However, certain operational differences remain. Fixed-broadband subscribers are easier to track down, as they are locked to a specific address, and the subscription is likely to have a name associated with it. Wireless users, by contrast, may move about freely, and often use

---

22 Navid Hassanpour, "Media Disruption and Revolutionary Unrest: Evidence From Mubarak's Quasi-Experiment," *Political Communication* 31, no. 1 (2014): 1–24.

23 Anita R. Gohdes, "Pulling the Plug Network Disruptions and Violence in Civil Conflict," *Journal of Peace Research* 52, no. 3 (2015): 352–67.

24 Anita R. Gohdes, "Information, Connectivity, and Strategic State Repression" (56th International Studies Association Conference, New York, 2015).

prepaid cards that do not necessitate identification when purchased. However, once identified, wireless users can be more easily tracked by triangulating cellphone tower signals, thus monitoring both position and movement. To circumvent such surveillance, users may choose to forego their own devices or subscriptions. State authorities are less able to identify and monitor suspected opposition members when these use open Wi-Fi networks or Internet cafés.

Authoritarian reversal

If in some circumstances, in certain countries, the diffusion of ICT can serve to augment the power of the state, it is not inconceivable that this technological change can affect the democratization of the states in question. When regimes consolidate and centralize their power, they can either arrest or reverse processes of democratization, leading to "authoritarian reversal." The literature on this topic has not directly addressed the issue of ICT, but some general findings might serve as a useful guide to thinking about the problem.

In general, we know from numerous studies that there is a positive relationship between economic development and democratization, though the reasons remain unclear.[25] There is also some evidence that the relationship works in reverse: low growth or economic recessions can retard or reverse democratization. Adam Przeworski[26] has argued that democracy is strong in developed countries but frail in poor ones because more income can be redistributed in the former than in the latter. Democracy in a developed country is thus a more robust equilibrium, because more redistribution can take place without endangering it.

Empirical studies add further nuances to this proposition. It has been held that "consolidated" democracies are practically immune to authoritarian reversal—but how can we know which democracies are truly consolidated, and which ones have simply survived for some period due to favorable circumstances? The age of a democracy might not be a good predictor of continued survival. To account for this lack of observability, Milan Svolik has devised various econometric models to measure threats to democracy. [27] He finds that previous models have underestimated the risk of early reversals while overestimating the risk of late reversals. He

---

25 Barbara Geddes, "What Do We Know about Democratization after Twenty Years?," *Annual Review of Political Science* 2, no. 1 (1999): 115–44.

26 Adam Przeworski, "Democracy as an Equilibrium," *Public Choice* 123, no. 3–4 (2005): 253–73.

27 Milan Svolik, "Authoritarian Reversals and Democratic Consolidation," *American Political Science Review* 102, no. 02 (2008): 153–68.

also finds that the only accurate predictor of reversal is economic recession. Therefore, what threatens the democratic equilibrium might not be the level of development per se, but any significant negative change in the basis for the economic distribution.

Despite these findings, economics are not the only predictor of democratization or reversals. Distinguishing between types of reversals, we find temporal variation in the risk. In a later study, Svolik argues that democracies consolidate against coups, but not incumbent takeover: "Put metaphorically, the risk of a coup appears to be a childhood disease: its danger disappears once a democracy survives long enough to consolidate. By contrast, the accumulation of too much power in the hands of an incumbent seems to be a persistent threat to democratic stability."[28] Truly consolidated democracies might thus be those that are sufficiently institutionalized to prevent both types of reversals.[29] Regime type might also matter, as presidential systems are more likely to experience reversal.[30]

We thus have two potential mechanisms for authoritarian reversal: economic recession, and the consolidation of executive power. The former might be relevant for the discussion here if cyber-attacks sufficiently damage the local economy—but that seems a rather farfetched scenario. Instead, the risk of incumbent takeover appears more relevant to the issue of building cyber-capacity. If democratic consolidation means institutionalization and thus decentralization of power away from the executive, building cyber-capacity can threaten this process. As the state becomes better able to monitor its population, repression becomes easier, all else being equal. Without appropriate and commensurate institutional checks on this new capacity, power then reverts back to the center. While the threat of authoritarian reversal is probably low across the board, under certain circumstances the risk might be more than negligible. The real or perceived threat to the incumbent regime may trigger repressive actions, in turn resulting in reversal or civil war, or both.

---

28 Milan W. Svolik, "Which Democracies Will Last? Coups, Incumbent Takeovers, and the Dynamic of Democratic Consolidation," *British Journal of Political Science*, 2012, 21.

29 Ethan B. Kapstein and Nathan Converse, "Why Democracies Fail," *Journal of Democracy* 19, no. 4 (2008): 57–68; Valerie Bunce, "Comparative Democratization Big and Bounded Generalizations," *Comparative Political Studies* 33, no. 6–7 (2000): 703–34.

30 Ko Maeda, "Two Modes of Democratic Breakdown: A Competing Risks Analysis of Democratic Durability," *The Journal of Politics* 72, no. 4 (2010): 1129–43.

Building cyber-capacity in practice

Given the various threats and risks discussed above, cyber-capacity building (CCB) is a difficult policy endeavor. It must serve to help minimize the threat of cyber-attacks and exploitation, while ensuring that recipient governments do not use the tools and capabilities to exert repression when faced with real or imagined political threats. In general, CCB is meant to prevent, detect, and handle cyber-incidents, with various organizations handling the various stages.[31] The components of CCB can be further divided into three categories: technological, human, and organizational resources. The first refers to hardware and software; the second, to the people who have the technical skills to use these tools; and the third, to building organizations and institutions to put all of these components together in a sensible and efficient manner.[32]

One of the most common forms of CCB is the formation of a national computer emergency response team (CERT).[33] Simply put, there are two types of CERTs: the radar model, and the rescue model.[34] The former involves direct monitoring of data traffic by placing sensors across networks. These sensors can detect malware, and can be used as early-detection systems for Internet service providers (ISP) and other critical infrastructure networks. This is the model currently used in Norway, where the sensor arrangement is voluntary and is publically acknowledged. The 'rescue' model is based on the active participation of key actors

---

31 In Norway, NorSIS works on the prevention side by advocating standards and good cyber-hygiene. Detection is done by the targeted organizations, other entities that observe malicious activity, or NorCERT through its sensor network across Norwegian networks. Handling is usually done by the targeted organizations, sometimes with the support of NorCERT.

32 Capacity can also be divided into different categories, such as human resources, organizational arrangements, and institutional and legal development. This report focuses more on technology and less on specific legal developments, since it is easier to generalize about the former than the latter. See: Patryk Pawlaki, "Developing Capacities in Cyberspace," in *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, ed. Patryk Pawlaki (Paris: ISSUE, 2014), 9–17.

33 There can be other government entities relevant for cyber-security. For instance, a national agency for coordinating cyber-policy and strategy across the government can help with inter-agency cooperation and ultimately strengthen capacity. However, the risks discussed in this report are most relevant to operational entities like a CERT.

34 Many thanks to Eldar Lillevik, Head of Department for Security Management at DNB, for this suggestion on how to conceptualize CERT models.

across the country. Instead of receiving signals from sensors, the CERT relies on companies, organizations, and individuals to provide information about malware and cyber-incidents. The CERT can then provide information to other actors at risk, while also helping the targeted actor handle the incident.

The technical and operational differences between these two models are readily apparent, but the key political distinction is one of *trust.* The radar model is possible in Norway thanks to trust and transparency between the government and society—but there are still limits to this trust, as evidenced by the contentious recent debate over the Data Retention Directive.[35] The radar model is probably not viable as an alternative in most other countries, particularly in those developing countries which have governments that are accountable to the public and that care about trust. The experiences of FIRST, a non-profit organization dedicated to CCB, lend support to this argument. FIRST does considerable work in developing countries helping to set up their first CERTs. However, the radar model is never on the agenda when working with these countries.[36] This is in part because FIRST does not support such surveillance, but it could also be that those countries seeking help do enjoy have the necessary public trust to use the radar model.

Some countries do use extensive data monitoring, and they are usually non-democratic. In addition to the countries discussed above (China and Syria), numerous other autocracies have structures in place to monitor and censor Internet traffic. Sensors are used in order to detect malware, but also to conduct deep-packet inspection for checking the content of data traffic, so that undesirable content can be catalogued and filtered out before it reaches the end-user. If we then assume that these states are directly connected to Internet switches and ISPs, the same organization can conduct surveillance of the population and control their Internet access (e.g. the Great Chinese Firewall).

Even without direct access to the ICT infrastructure, states in developing countries may possess significant capabilities. The Israel–Palestine conflict has assumed new dimensions in recent years, with hackers on both sides launching cyber-attacks and stealing sensitive information. In 2014 during the Gaza War, various groups attacked Israeli government networks. The campaign included a wide range of actions, including simple Distributed Denial of Service attacks and the leaking of

35 Phone interview with Ivar Kjærem, Chief Security Officer at the Norwegian Cyber Defense Force, August 21, 2015.

36 Phone interview with Margrete Raaum, FIRST chairwoman of the board July 23, 2015.

several databases.[37] After the regular military operation ended, the cyber-conflict continued, with both sides stealing and leaking sensitive information. According to a Palestinian security official, Palestinian security officials stole files from an Israeli security agency containing the identities of dozens of agents recruited by Israeli intelligence.[38] While third-party actors have participated in these operations, there should be no technical reason why these endogenous capabilities could not be used against the domestic population, and not only against outside actors.

In some cases, these capabilities come from the private sector. Private cyber-security firms are part of a booming industry, and states can buy malware tools from various companies. After the hacking of the Italian company Hacking Team's servers, it was revealed that the Ethiopian government had received training for hacking and access to the company's spy tools as part of a $1 million contract.[39] The Ethiopian Information Network Security Agency (INSA) then used the tools to spy on people associated with the political opposition and even US-based journalists. Hacking Team has also sold its services to numerous other countries known for systematically violating human rights, including Egypt, Sudan, and Azerbaijan.[40]

Given the potential risks associated with these technical capabilities, CCB should focus primarily on organizational development and building human resources. When FIRST starts working with a country, it usually does not start from scratch. There will be some committed officials or politicians dedicated to addressing the problems, but they lack formal

---

37 Gilad Zahavi, "#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation," *SenseCy Blog*, August 11, 2014, http://blog.sensecy.com/2014/08/11/opsavegaza-campaign-insights-from-the-recent-anti-israel-cyber-operation/; Armin Rosen, "Israel Faced A Huge Wave Of Cyber Attacks During Its War With Hamas — And Iran Could Be The Reason Why," *Business Insider*, August 18, 2014, http://www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8.

38 Adnan Abu Amer, "Hamas' Cyber Battalions Take on Israel—Al-Monitor: The Pulse of the Middle East," *Al-Monitor*, July 29, 2015, http://www.al-monitor.com/pulse/originals/2015/07/palestine-israel-internet-cyber-war-hacking.html.

39 John Leyden, "Hacking Team Mulled Stopping Ethiopia Sales—because of Idiot G-Men," *The Register*, August 17, 2015, http://www.theregister.co.uk/2015/08/17/hacking_team_ethiopia/.

40 Cora Currier and Morgan Marquis-Boire, "A Detailed Look at Hacking Team's Emails About Its Repressive Clients," *The Intercept*, July 7, 2015, http://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

structures like a CERT.[41] There will also be a lack of people skilled in cyber-security. FIRST then helps with training people and setting up the necessary incident-response teams. However, technical training is only the initial step in building capacity. In fact, this component is one of the easiest parts—building control mechanisms (e.g. formal oversight) and organizational structure requires skills that span a wide range of disciplines and are thus much harder to achieve.[42]

CCB should use an integrative approach to include as many actors as possible, in order to achieve systematic and enduring cyber security.[43] However, integration is particularly challenging, because it involves people from different backgrounds and agencies.[44] If a CERT has coordinating responsibility across the government, and even with the private sector, it must interact with everyone from diplomats to corporate executives. Thus, we must consider both the internal components of cyber-security agencies and their interface with other organizations.[45]

Exactly what a new CERT should look like depends on the needs and resources available. At a minimum, a rescue CERT may consist of one secretary with an email list.[46] Once the CERT receives notice of a cyber-incident, that secretary can then forward the information to relevant actors. The more complex the infrastructure and the larger the threat, the greater the organizational requirements become for the CERT, for several reasons. First, since cyber-attacks can cause damage across sectors due to interdependence, the need for information-sharing becomes paramount. The informational complexity of certain cyber-attacks can be too great for one actor to handle alone.[47] Also, some companies might not want to or be able to speak directly to other companies, so they will have to rely on a central hub to spread information. Second, some companies might not have the technical capabilities to handle particularly complex

41 Interview with Margrete Raaum, July 23, 2015.

42 Phone interview with Ivar Kjærem, August 21, 2015.

43 Neil Robinson, "Building Blocks for Strengthening Cybersecurity Capacities," in *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, ed. Patryk Pawlaki (ISSUE, 2014), 64.

44 Ibid., 62.

45 This model draws heavily on Robinson's conceptualization of a "connected continents" model of CCB, but leaves open the question of format and whether hierarchy or network is most appropriate. See: Ibid., 67–68.

46 Interview with Eldar Lillevik in Oslo, July 6, 2015.

47 Hans-Inge Langø, "Conflict in a Privatized Domain: Assessing Situational Awareness and Decision- Making in Cyberspace" (International Studies Association, Toronto, 2014).

incidents. With sufficiently trained staff, the CERT can then help them handle these incidents.

In addition to considering the organizational requirements of such entities, we must also think about their placement and relationship with others. For a national CERT, this is a tricky balancing act. It must be in a position of influence, to remain politically relevant—but it must also be relatively autonomous, to avoid being co-opted by security services and used for repressive purposes.[48] Such co-optation might not even be intentional or aimed at changing the purpose of the CERT. By placing it under or close to a security service, the organizational culture of the latter could influence the former so that offense takes precedence over defense.

While these risks are real, the organizational aspect of CCB also carries potentially significant benefits. If a CERT or other cyber-security entities are formally established within the government structure, this process can help institutionalize authority and thus prevent co-opting. Further down the line, this process can help build legitimacy for the government, promoting trust between it and the population. However, achieving these goals might necessitate there being some political institutions to begin with: institutions might be both a precondition for and a consequence of CCB. It is essential to think carefully about CCB itself and the level of institutionalization, and thus legitimacy and democracy, in the receiving state itself.

This dilemma became evident in Myanmar in 2014. Qatar's Ooredoo and Norway's Telenor were licensed to help build up Myanmar's telecommunications infrastructure. The World Bank pledged $2 billion in development aid to help build and reform the sector.[49] However, critics raised serious questions about the lack of responsible investments. In a letter addressed to the World Bank, several dozen non-profit organizations argued that the new reform project ignored "fundamental issues of privacy, human rights, and surveillance."[50] The organizations claimed that the World Bank had not prioritized these issues, and that recent My-

48 Interview with Lillevik, July 6th, 2015.

49 Rachel Wagley, "Telecom Investments Threaten Privacy Rights in Burma," *DVB Multimedia Group*, February 4, 2014, https://www.dvb.no/analysis/telecom-investments-threaten-privacy-rights-in-burma-myanma/36706.

50 "Civil Society Comments: World Bank Telecom Sector Reform Project, Burma" (U.S. Campaign for Burma, January 21, 2014), 2, http://uscampaignforburma.org/images/Civil_Society_Comment_on_the_World_Bank_Telecom_Sector_Reform_Project_in_Burma.pdf.

anmar legislation did not restrain the state from abusing its power: "failure to address privacy and security issues while expanding connectivity and providing technical support and training may further empower the government to engage in surveillance, censorship, and other abuses."[51] This case makes clear the need for investments to go hand-in-hand with institutional reform.

Governmental cyber-security entities also have to relate to organizations outside the state. This aspect of CCB, commonly referred to as public–private partnerships (PPPs), can help build trust and institutionalize cyber-security. By no means a panacea, PPPs are still essential because in most countries much of cyberspace is either owned or operated by private-sector companies. For a CERT, the private sector is both a recipient of aid and a source of information, and CCB must help build these relationships.

Another dimension often neglected in CCB is the role of civil society and non-governmental actors. There are a great many voluntary actors helping both governments and private companies to become better at cyber-security. These actors range from formal organizations like FIRST, to informal networks of technical experts who exchange information about vulnerabilities and incidents. As many developing countries lack the capital and the human resources needed for adequate defense against the many threats in cyberspace, governments should look to build capacity externally as well as internally. Some countries have even decided to incorporate private citizens into the cyber-defense infrastructure. The Estonian Defense League, a voluntary national defense organization, has a separate cyber-defense unit consisting of specialists from the public and private sectors who can be mobilized in the event of a crisis. Although there are possible command-and-control issues with such a structure, it is an undeniable fact that many of the brightest talents often make their living outside of the government.

An added advantage of such partnerships is that they help keep power decentralized, and, in theory at least, reduce the risk of repression. Yes, centralized state power can be abused and directed against the population. But if the private sector and volunteer actors become part of

51 Ibid.

the security structure, the government becomes reliant on them to maintain cyber-security functions. In essence, the partners become veto players who can challenge policies perceived as illegitimate.[52]

52 This assumes that the government would not use force or the threat of force to maintain partnerships, in which case we would be dealing with vastly different situations.

Policy implications

As this report has shown, there are risks associated with building cyber-capacity. While cyber-security will only grow in importance, for both the economy and society at large, information communications technology as such is value-neutral. Under certain circumstances, its positive potential may be outmatched by the actions of actors with malicious intentions. Those actors may represent the state or some other organization, but this report has primarily focused on the former, as they are the recipients of CCB aid. From the government perspective, ICT is truly a dual-use purpose: it may be used both to protect and to oppress. The risk of repression is nontrivial, but—importantly—it is not uniformly distributed amongst developing countries. Some countries are at greater risk than others, so a major implication of this report is that CCB policies must be tailored to each individual recipient country.

Donor countries should be wary of contributing technical tools. Instead, efforts should focus on building organizations and institutions. However, this is also slightly paradoxical, as the best way to safeguard against repression is the presence of government institutions that promote accountability and create legitimacy. Many developing countries lack these institutions—particularly within cyber-security, since this is a relatively new area of responsibility for governments. Donor countries should help build institutions along with capacity, as the latter without the former may serve to enable repression. At worst, increased capacity may even encourage repression, if the state centralizes power and strengthens the executive. Here it might be instructive to consider lessons from experience with security sector reform, where efforts in Afghanistan and elsewhere have triggered similar dilemmas as those described here.[53]

In terms of practical recommendations, donors should help recipients build national CERTs that coordinate between government agencies and between the government and the private sector, particularly owners and operators of critical national infrastructure. Donors may even help facilitate this cooperation, for instance by connecting governments with the

53 For a review of some of the dilemmas associated with security sector reform, see Michael Brzoska, "Introduction: Criteria for Evaluating Post-Conflict Reconstruction and Security Sector Reform in Peace Support Operations," *International Peacekeeping* 13, no. 1 (2006): 1–13.

private sector abroad, such as telecommunications companies. Informal gatherings can be a good way of sharing best practices and building trust among and between organizations, which is an essential prerequisite for information-sharing on threats and vulnerabilities.

Bibliography

Amer, Adnan Abu. "Hamas' Cyber Battalions Take on Israel—Al-Monitor: The Pulse of the Middle East." *Al-Monitor*, July 29, 2015. http://www.al-monitor.com/pulse/originals/2015/07/palestine-israel-internet-cyber-war-hacking.html.

Bilbao-Osorio, Benat, Soumitra Dutta, and Bruno Lanvin. "The Global Information Technology Report 2014." Geneva: World Economic Forum, 2014.

Brzoska, Michael. "Introduction: Criteria for Evaluating Post-Conflict Reconstruction and Security Sector Reform in Peace Support Operations." *International Peacekeeping* 13, no. 1 (2006): 1–13.

Bunce, Valerie. "Comparative Democratization Big and Bounded Generalizations." *Comparative Political Studies* 33, no. 6–7 (2000): 703–34.

"Civil Society Comments: World Bank Telecom Sector Reform Project, Burma." U.S. Campaign for Burma, January 21, 2014. http://uscampaignforburma.org/images/Civil_Society_Comment_on_the_World_Bank_Telecom_Sector_Reform_Project_in_Burma.pdf.

Currier, Cora, and Morgan Marquis-Boire. "A Detailed Look at Hacking Team's Emails About Its Repressive Clients." *The Intercept*, July 7, 2015. http://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

Davenport, Christian. "State Repression and Political Order." *Annual Review of Political Science* 10 (2007): 1–23.

———. "Understanding Covert Repressive Action The Case of the US Government against the Republic of New Africa." *Journal of Conflict Resolution* 49, no. 1 (2005): 120–40.

Fein, Helen. "More Murder in the Middle: Life-Integrity Violations and Democracy in the World, 1987." *Human Rights Quarterly* 17 (1995): 170.

Geddes, Barbara. “What Do We Know about Democratization after Twenty Years?” *Annual Review of Political Science* 2, no. 1 (1999): 115–44.

Gohdes, Anita R. “Information, Connectivity, and Strategic State Repression.” New York, 2015.

———. “Pulling the Plug Network Disruptions and Violence in Civil Conflict.” *Journal of Peace Research* 52, no. 3 (2015): 352–67.

Hassanpour, Navid. “Media Disruption and Revolutionary Unrest: Evidence From Mubarak’s Quasi-Experiment.” *Political Communication* 31, no. 1 (2014): 1–24.

International Telecommunications Union. *Measuring the Information Society Report 2014*. Geneva: International Telecommunications Union, 2014.

Kapstein, Ethan B., and Nathan Converse. “Why Democracies Fail.” *Journal of Democracy* 19, no. 4 (2008): 57–68.

Kelly Garrett, R. “Protest in an Information Society: A Review of Literature on Social Movements and New ICTs.” *Information, Communication & Society* 9, no. 02 (2006): 202–24.

King, Gary, Jennifer Pan, and Margaret E. Roberts. “How Censorship in China Allows Government Criticism but Silences Collective Expression.” *American Political Science Review* 107, no. 02 (2013): 326–43.

Langø, Hans-Inge. “Conflict in a Privatized Domain: Assessing Situational Awareness and Decision- Making in Cyberspace.” Toronto, 2014.

Lawrence, Japhet Eke, and Usman A. Tar. “Barriers to E-Commerce in Developing Countries.” *Information, Society and Justice Journal* 3, no. 1 (2010): 23–35.

Leyden, John. “Hacking Team Mulled Stopping Ethiopia Sales—because of Idiot G-Men.” *The Register*, August 17, 2015. http://www.theregister.co.uk/2015/08/17/hacking_team_ethiopia/.

Lynch, Marc. “After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State.” *Perspectives on Politics* 9, no. 02 (2011): 301–10.

Maeda, Ko. “Two Modes of Democratic Breakdown: A Competing Risks Analysis of Democratic Durability.” *The Journal of Politics* 72, no. 4 (2010): 1129–43.

Meier, Patrick Philippe. “The Impact of the Information Revolution on Protest Frequency in Repressive Contexts,” 15–17. New York, 2009.

Morgan, Steve. “Cyber Crime Costs Projected To Reach $2 Trillion by 2019.” *Forbes*, January 17, 2016. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/.

Pawlaki, Patryk. “Developing Capacities in Cyberspace.” In *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, edited by Patryk Pawlaki, 9–17. Paris: ISSUE, 2014.

Pierskalla, Jan H., and Florian M. Hollenbach. “Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa.” *American Political Science Review* 107, no. 02 (2013): 207–24.

Przeworski, Adam. “Democracy as an Equilibrium.” *Public Choice* 123, no. 3–4 (2005): 253–73.

Regan, Patrick M., and Errol A. Henderson. “Democracy, Threats and Political Repression in Developing Countries: Are Democracies Internally Less Violent?” *Third World Quarterly* 23, no. 1 (2002): 119–36.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.

Robinson, Neil. “Building Blocks for Strengthening Cybersecurity Capacities.” In *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, edited by Patryk Pawlaki, 18–27. ISSUE, 2014.

Rød, Espen Geelmuyden, and Nils B. Weidmann. “Empowering Activists or Autocrats? The Internet in Authoritarian Regimes.” *Journal of Peace Research* 52, no. 3 (2015): 338–51.

Rosen, Armin. “Israel Faced A Huge Wave Of Cyber Attacks During Its War With Hamas — And Iran Could Be The Reason Why.” *Business Insider*, August 18, 2014. http://www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8.

Shapiro, Jacob N., and David A. Siegel. “Coordination and Security How Mobile Communications Affect Insurgency.” *Journal of Peace Research*, 2015, 0022343314559624.

Shapiro, Jacob N., and Nils B. Weidmann. “Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq.” *International Organization* 69, no. 02 (2015): 247–74.

Spector, Regine, and Andrej Krickovic. “Authoritarianism 2.0: Non-Democratic Regimes Are Upgrading and Integrating Globally.” San Francisco, 2008.

Svolik, Milan. “Authoritarian Reversals and Democratic Consolidation.” *American Political Science Review* 102, no. 02 (2008): 153–68.

Svolik, Milan W. “Which Democracies Will Last? Coups, Incumbent Takeovers, and the Dynamic of Democratic Consolidation.” *British Journal of Political Science*, 2012, 1–24.

International Telecommunications Union. *The World in 2014: ICT Facts and Figures.* Geneva: International Telecommunications Union, 2014.

Wagley, Rachel. “Telecom Investments Threaten Privacy Rights in Burma.” *DVB Multimedia Group*, February 4, 2014. https://www.dvb.no/analysis/telecom-investments-threaten-privacy-rights-in-burma-myanma/36706.

Zahavi, Gilad. “#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation.” *SenseCy Blog*, August 11, 2014. http://blog.sensecy.com/2014/08/11/opsavegaza-campaign-insights-from-the-recent-anti-israel-cyber-operation/.

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the Author

Hans-Inge Langø is a Phd student at the Department of Government at the University of Texas at Austin. He holds an MA in International relations from Boston university. Mr. Langø has previously worked as a junior research fellow at the Norwegian Institute of International Affairs, having spent several years researching the strategic implications of cyber security from both a national and international perspective. He also has experience working on various US foreign policy issues in Washington, DC, including providing analysis of defense spending and procurement programs to two task forces. His current research focuses on third-party interventions and civil wars.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no