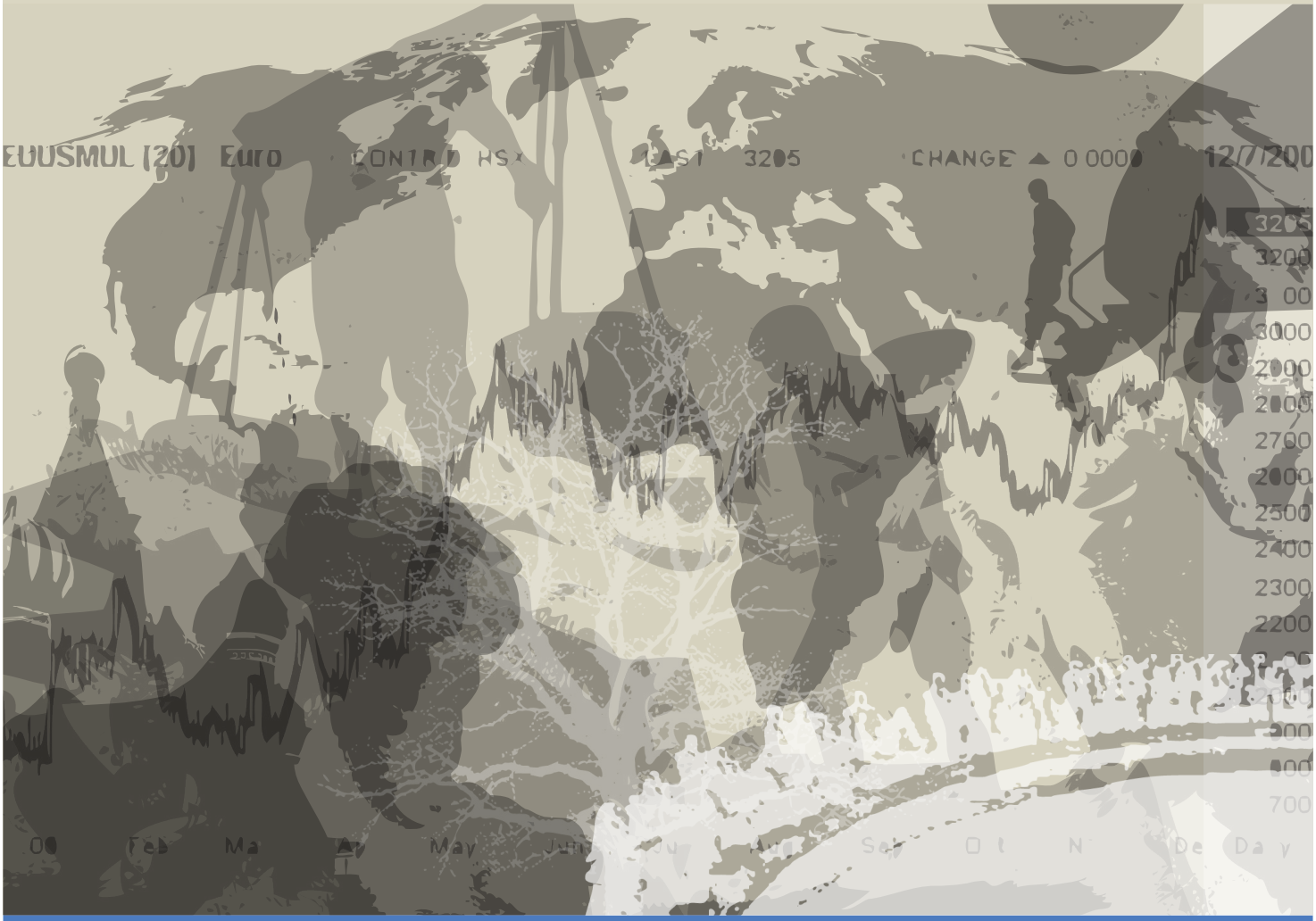
Norwegian Institute of International Affairs

Cyber Security Capacity Building: Developing Access

Alexander Klimburg and Hugo Zylberberg



NUPI Report
[Report no. 6, 2015]

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

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: Developing Access

Alexander Klimburg and Hugo Zylberberg

Published by Norwegian Institute of International Affairs

Table of Contents

Introduction

The rise of cyber security as an important factor in international relations has taken on many guises. Originally mostly an economic issue, it was quickly followed by international security agendas, and, in recent years, a lively debate on human rights. The *developmental* context is a relative newcomer to this field. The key instrument connecting the various discourses is increasingly referred to as Cyber Security Capacity Building (CCB), and, although only few governments today maintain such programmes (often accounting for a tiny fraction of overall aid flows), CCB seems set to play an important role in future foreign policy considerations.

There are three principle reasons why CCB is likely to grow in importance. Firstly, it is becoming increasingly clear that a key factor in economic and social development (and therefore political stability) is access to cyberspace. In turn, cyber security becomes a key ingredient for promoting this access, and ensuring that it is not jeopardized through predatory criminal behaviour. Secondly, given the nature of the Internet, if countries in the rich industrialized world are to be able to respond to cyber-threats against their own citizens, increasing cooperation is needed with the developing world – which increasingly hosts the infrastructure and indeed the actors behind malicious cyber activity. Such cooperation can be possible only if basic cyber security institutions and skills are present in the partner countries – which is very much in the direct interest of donor countries. Thirdly, the increasingly politicized global struggle for dominance over governance of the Internet makes the issue of overriding importance within international relations. With two opposing views emerging on how the Internet should be governed, the importance of the 'swing states' – nearly all within the developing world – also grows. While the present study does not advocate using CCB as a bargaining chip in international diplomacy, the 'soft power' aspect of aid in general (and CCB in particular) should not be ignored. Given this triple rationale (regional stability, national security, and international diplomacy), CCB may well become one of the most important activities within the security/development nexus in the future.

This study concentrates on providing the rationale and identifying potential 'dimensions' for such governmental CCB instruments, and what tasks they should cover. The 'methodological' dimension includes developing frameworks for assessing and delivering CCB programmes, but also extends to general frameworks for supporting a country's national cyber security strategy – as well as the basic research needed. The 'technical' dimension is concentrated on the need to train and support the Computer Emergency Response Team (CERT) and law-

enforcement capabilities of partner countries. In fact, such initiatives had already been ongoing for many years before the term 'CCB' was coined. Thirdly, the existence of 'infrastructure' development programmes has long been a feature of international development, albeit without much focus on security concerns. Fourthly, the instrument of overall 'budgetary support' can be used for directly funding partner countries' operational expenses in issues related to cyber security over a prolonged period.

The study concludes with some recommendations for policy-makers.

1. Cyber Security Capacity Building (CCB): Developing access

The Internet provides a major developmental opportunity for the Global South, or the 'developing world'. As noted in a recent World Economic Forum report (WEF, 2015), in 2014, emerging markets were home to 96% of all the human beings who were *not* connected to the Internet and the 'digital economy.' As defined by the WEF, the digital economy is that part of the economy made possible by the fact that 'almost 3 billion connected consumers and businesses search, shop, socialize, transact and interact every day using personal computers (PCs) and, increasingly, mobile devices.'[1] This digital economy 'contributed $2.3 trillion to the G20's GDP in 2010 and an estimated $4 trillion in 2016, [and] is growing at 10% a year – significantly faster than the overall G20 economy' (WEF, 2015). In emerging markets, the annual growth rate of the digital economy ranges between 15 and 25%, greatly outstripping growth rates in the developed world. There is growing evidence that the increased use of ICT – including Internet access – is a significant driver of growth in the developing world. Indeed, some research indicates that in the first decade of the millennium alone, up to one fourth of the growth in developing countries derived from the deployment of ICT – a trend expected to accelerate in the second decade (ITIF, 2012). The World Bank (IC4D, 2009) has found that a 10% increase in high-speed broadband Internet penetration adds 1.38% to annual per capita GDP growth in developing countries. Likewise, a 10% increase in mobile phone penetration adds 0.81% to annual per capita GDP growth in developing countries (IC4D, 2009). Clearly, ICT is rapidly becoming not only a key factor in promoting development and therefore stability, but perhaps the single most important factor.

Cyber Security Capacity Building (CCB) represents one approach to fostering ICT-led growth and stability in developing countries. Unlike other developmental approaches, it is concerned primarily (although not exclusively) with security-related issues. As is the case with many security issues, it has not been universally defined and different countries use different holistic approaches to CCB. The Foreign and Commonwealth Office's (FCO) goals[2] for their CCB programme derive directly from the national goals of the UK National Cyber Security Strategy (UK Cabinet Office, 2011) –transposed into an overseas development framework. On the other hand, the cyber security strategy of the EU (JOIN, 2013) mentions the development of norms of government behaviour, the economic prospects of growth and security issues, and is

1 Figure from Euromonitor International, 2014

2 See Box 6

explicitly principles-based: 'The EU's core values apply as much in the digital as in the physical world.' These values include 'Protecting fundamental rights, freedom of expression, personal data and privacy' as well as 'Access for all' and 'Democratic and efficient multi-stakeholder governance'.

CCB is a recent addition to the security/development nexus. In comparison to other security and development issues, like Security Sector Reform (SSR), or Disarmament, Demobilization and Re-Integration (DDR), CCB stands out as much more connected to the broader economic landscape, with security issues that are even more immediately cross-border, and deals with overall issues that are (arguably) much more complex in width (thematic reach) and depth (technical detail).

This section presents what we believe to be the underlying rationale for supporting CCB at the political level. Firstly, CCB can assist in economic development, thereby helping to promote stability in the developing country. Secondly, CCB can help bring partner and donor countries closer together in the evolving international cyber security architecture, with tangible effects on the security of donor countries. Thirdly, CCB can help promote and enhance freedom on and through the Internet by encouraging participation in Internet governance.

1.1 Promoting access to economic growth through an enabling business environment

Economic growth contributes to political stability, and ICT plays an ever-growing role in growth. As noted by the World Economic Forum report (WEF, 2015), recent annual growth in the digital economy ranges between 15 and 25%, but to realize the potential impact on economic growth, emerging markets face two challenges: expanding their network coverage, and building their network capacity.

Expanding network coverage

As an increasing literature on the impacts of broadband shows, widely available broadband has a significant impact on GDP growth. As noted by the World Bank (IC4D, 2012), it 'deserves a central role in country development and competitiveness strategies'; moreover, with every 10% increase in penetration, broadband is associated with an additional 1.38% increase in GDP – a figure widely quoted in the subsequent literature. In the more recent report of the International Telecommunications Union (ITU, 2012), the authors 'validate the positive contribution of broadband to GDP growth for developing countries and regions' and point to the 'clear return to scale effect'. In countries with high broadband penetration, 1% growth in broadband penetration results in an increase of between 0.023 and 0.026% in GDP growth. In countries with low broadband penetration, the contribution to GDP growth ranges between 0.008 and 0.021%. Furthermore, the economic benefits of network coverage are not limited to growth: they are signifi-

cant for creating employment as well. However, the ITU report (2013) also offers detailed analyses indicating that countries first need to build a critical mass – businesses capable of thriving in an Internet-enabled environment – in order to experience the benefits of network coverage.

Building network capacity

Dalberg (2013) points to the fact that 'no vibrant Internet economies (...) have been built atop poor business environments'. Keys to a better business environment include not only the availability of the infrastructure, but also the adequacy of backbone network infrastructure, network ownership and geographic patterns of network development (IC4D, 2009).

Concerning backbone infrastructure, in sub-Saharan Africa, only 12% of the infrastructure is fibre-optic cable (IC4D, 2009); the rest is microwave. Even if the share of fibre-optic varies across countries and operators, this overall low capacity is inadequate to support thriving mass market connectivity. The situation is 'the opposite of that in more advanced markets, where fibre-optic backbone networks dominate and wireless technologies are used as backbone infrastructure primarily in remote and inaccessible areas.'

As regards ownership, vertical integration of businesses leads to low levels of competition over infrastructures: there is 'little wholesale trading of backbone services' (IC4D, 2009). This provides few incentives for operators to increase their delivery capacities; moreover, the ability to prevent other operators from using their own infrastructure prevents the markets from exploiting the economies of scale.

Finally, as to the geographical distribution of services, and given the lack of competition and the high fixed costs of developing such networks, fibre-optic backbone networks are located mostly in or between urban areas. Arguments for or against 'net neutrality' aside,[3] with most of the Internet content accessed by developing countries being located outside the region, greater demand for the Internet is likely to lead to increased development of network capacity towards other countries.

There are therefore very few incentives for local actors to either build network capacity in mostly rural areas or to expand network coverage. Development efforts need to focus on bridging this infrastructural gap, as a key determinant in an enabling business environment.

---

3 Telcos worldwide – and especially among many developing countries – have lobbied for the ability to charge Internet companies (such as Google, Facebook and Netflix) selectively for their use of telcos' networks. Within the developing world this discussion has distinct anti-colonial overtones, and is referred to as an Internet 'tax'.

Security and cybercrime

Development efforts should also focus on the risks associated with cybercrime, for three reasons. Firstly, the security/development nexus is increasingly recognized as a key component of both security and development efforts. Secondly, CCB activities should have a deeper focus on cyber security, because the areas with the highest potential of economic growth correspond roughly with those where the security risks are the highest. Thirdly, the skills developed locally through cyber security trainings correspond to those needed to enable local businesses to scale up, without having to rely on outside, more expensive talent.

The security/development nexus

The crucial importance of the security/development nexus is increasingly recognized by the security and the development communities alike. As early as 1999, UK Secretary of State for International Development, Clare Short, identified SSR as a prerequisite for sustainable development, and (in DCAF/ISSAT, 2012), the concept of SSR 'explicitly emphasized the linkages between security and development, prompting the development community to redefine its role in the field of security, while also highlighting the importance of security in the establishment of sustainable peace and development'.

It is broadly acknowledged that SSR is:

- 'A Nationally-Owned process aimed at ensuring that security and justice providers deliver': transposed to the cyber world, this expresses the need for methodological support to develop a National Cyber Security Framework relying for example on the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) framework of Box 1.

- 'Effective and Efficient security and justice services that meet the people's needs': transposed to the cyber world, this expresses the need for technical support to develop CERT and Law Enforcement capabilities and their ability to cooperate.

- '[Accountability of the security and justice providers] to the State and its people, operating within a framework of good governance, rule of law and respect for human rights': transposed to the cyber world, this calls for a broader methodological support not only addressing cyber issues but more broadly strengthening democratic governance, transparency and accountability, in order to further the goals of CCB activities (DCAF/ISSAT, 2012).

Cyber security

The principal Internet contributions to overall economic growth are also those most vulnerable to cybercrime. One survey (Dalberg, 2013) of 1300 business (among which nearly 1000 small and medium-sized enterprises (SMEs)) in the developing world identified three main areas where it was crucial to address cyber security from the start:

1. Backend systems (e.g. ERP systems such as SAP or similar) can unlock significant growth in helping SMEs as well as government deal with management challenges. As Dalberg notes, 'cost savings from enterprise systems, for example, have delivered 30% savings for national health insurance schemes'. However, those enterprise systems concentrate the company's information in one place, making it more vulnerable to potential hackers, who can steal vast quantities of data in one single hacking operation. Any move to a 'paper-less office', in government ('e-government') and in the private sector, must therefore place a high premium on cyber security.

2. With higher-bandwidth intensive Internet solutions and the decreasing costs of mobile broadband plans – currently representing an impressive 11.3 to 24.7% of monthly gross national income per capita – cloud-computing is likely to develop and further this concentration of information. The deployment of cloud-based solutions for managing data and providing IT solutions may lead to a 'leapfrogging' over certain more traditional ERP-system deployment – and the corresponding cyber security needs will be different.

3. The spread of mobile money and eCommerce will provide another incentive for thieves to develop cybercrime schemes. E-banking theft is very much an issue in the developed world, but not yet in the developing world – and this gap will close with increased sophistication. Similarly, the deployment of innovative mobile or Internet money approaches and more traditional credit or debit card-based e-commerce solutions has attracted online fraudsters. Online crime can greatly harm consumer trust; if not addressed, these security concerns could curtail development in those sectors. Unlike in Europe and North America, in the emerging markets both the services and the crime are being introduced simultaneously, so appropriate cybercrime legislation and measures must be in place from the very start. In Europe, 'cybercrime legislation (...) was on few minds until fraud began.' Today emerging markets do not have that luxury.

Besides the three areas identified above, one further risk element can be noted: *reputational*. If a country or region becomes a noted haven for internationally-operating cybercriminals, it can suffer repercussions, with greater difficulties in doing business abroad, and even an

impact on levels of FDI. Also, as a survey from Nigeria has shown (Citizen Lab, 2013), cybercrime gangs are not above fleecing their own – especially when the international returns start to diminish. The study found that nearly half of all Nigerians claimed to have fallen victim to cybercrime, with financial repercussions, in 2012. The International Data Group Connect estimates that annually, cybercrimes cost the South African economy $573 million, the Nigerian economy $200 million, and the Kenyan economy $36 million: money that these countries can ill afford to lose. Addressing cyber security issues is therefore crucial from an early stage, before the costs associated with breaches slow down economic development.

Evaluating the cost of cybercrime in developing countries is a challenge, mainly because 'in the developing world (...) most governments do not collect any data on cybercrime at all' (McAfee, 2014) This study reports figures from countries that currently track cybercrime within their borders: 0.14% for Colombia, 0.01% for Kenya, 0.18% for Malaysia, 0.08% for Nigeria, 0.14% for South Africa, 0.13% for Vietnam, 0.19% for Zambia. These figures are extremely unlikely to be accurate; the same study averages losses for the developing world (including Nigeria) at around 0.2% of GDP ('high-income countries lost more as a percent of GDP, perhaps as much as 0.9% on average'). Still, this needs to be compared with the results of the Nigerian survey quoted above, which calculated that in 2012 cybercrime had cost the Nigerian economy around USD 12 *billion* in total (The Citizen Lab, 2013). While these figures should be approached with caution, the discrepancies do give food for thought.

Skills

'After access to high-bandwidth telecommunications infrastructure, the availability of employable talent is the single most important determinant for the growth of the IT services and ITES (IT-Enabled Services) industries in the long term' (IC4D, 2009). As McKinsey Global Institute reports quoted in (IC4D, 2009), based on a 2007 study in 28 developing countries: 'on average, only about 13% of generalist graduates had the necessary qualifications (including language) for being employed in the sector.' 'Willingness to work in the industry' and 'Trainability' are other key characteristics of the talent pool. These are skills that are enhanced by cyber security trainings, which thus serve the dual purpose of enhancing cyber security as well as opening new economic opportunities for local businesses.

A recurrent point noted in the interviews conducted for the present study is the importance of embedding cyber security skills early on, in the development phase. Indeed, much of the technical training provided by donor countries' CERTs aims at spreading the best practices of what can be called *secure coding*: teaching technical teams in partner countries to develop programmes and software that can minimize cyber security risks. In its 2010 research report, Carnegie Mellon's CERT®

identified *secure coding* as one of its main activities: working with 'software developers and software development organizations to reduce vulnerabilities resulting from coding errors before they are deployed.'

A key shortcoming of a purely economic approach is that the absence of locally-owned infrastructures leads to international players dominating the market, providing few incentives to address the challenges mentioned above. Local economic actors benefit little from development efforts when the infrastructure is not locally owned, as it is the international owners that capture most of the economic benefits. All reports stress the importance of relying on local providers, so that funding can stay in the partner-country economies, with a multiplier effect: money that remains in the local economies can then be re-used locally by those actors, promoting a virtuous economic circle. Donor countries need to view their benefits not only from an economic perspective, but from a political one as well.

1.2 Encouraging openness and freedom on the Internet through enhanced participation in Internet governance

The governance of the Internet is currently managed by self-organizing groups, with more or less equal weight to governments, the private sector and civil society. This approach has been called the *Multi-Stakeholder Model* (MSM) and is supported by most liberal democracies. However, other actors argue that state stability is paramount: they reject this model, calling for more power for governments, a view that can be described as *towards cybersovereignty*. The international dialogue over Internet issues has been polarized in the past few years between these two positions.

At the 2012 World Conference on International Telecommunications (WCIT) in Dubai, sponsored by the ITU, debates on the future of Internet governance saw, in the words of Alexander Klimburg (2014), 'a mass of (mostly developing) countries following Russia's lead and voting for a text that seemed to leave the door open for greater government involvement in the running of the Internet. Eighty-nine countries signed the documents, which critics said was a significant threat to the multi-stakeholder approach'. To create the necessary conditions for greater engagement in Internet governance among developing countries, advocates of the MSM should build the capacity for partner countries to participate more fully in Internet governance and promote human rights, good governance and the rule of law, in order to foster liberal democratic environments where all stakeholders can have incentives to engage internationally.

Building the capacity to participate fully in Internet governance

To promote their political positions on a free and open Internet, MSM advocates need to be more aware of the incentives for developing coun-

tries to support their views – not least, concerning the challenges of access and helping the developing countries to 'realize the promise of the Internet', as put by the Rwandan Minister of Telecommunications, Jean Nsengimana, at NETmundial in 2014. Supporting Internet capacity development through infrastructural, technical and social projects is the direct answer to questions of access.

CCB should make it possible for such countries to participate more fully in the field of Internet governance. After all, it is in the interest of partner countries to support the MSM once the conditions for an enabling business environment have been realized, based on the development of capacities within the private sector and civil society. This is the virtuous circle of the open Internet, which can enable a better business environment, with the emergence of local actors who themselves have incentives to support the open Internet from which they derive value.

Participating in Internet governance is largely a logistics question – for civil society as well as governmental actors. The many physical meetings involved – often spread across the globe – and the often arcane technical issues rule out engaging only 'part-time' in this space. Both governments and civil society actors in the developing world are often challenged by the inability to provide full-time staff and meet their logistic (travel) needs. This is clearly an area where donor countries can accomplish much, at relatively low cost.

Promoting human rights, good governance and the rule of law

Another political goal of CCB should be to promote the rule of law, good governance and human rights, which are likely to enable better business environments as well as leading to increased cooperation in Internet governance. As Maria Grazia Porcedda has noted (EUISS, 2011): 'human rights and good governance (...) as well as cyber security can be fostered by reshaping cyberspace in accordance with internationally endorsed principles of the rule of law'. Those conditions are crucial for the realization of economic growth, and they are at the heart of many of the CCB models that have already been established.

The EU's cyber security strategy (JOIN, 2013) emphasizes these issues. Putting access for all at the centre ('Everyone should be able to access the Internet and to an unhindered flow of information'), it establishes three international goals: 'promote openness and freedom (...), encourage efforts to develop norms of behaviour and apply existing laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cyber security capacity.' On this last point of capacity building, the strategy adds that 'the EU will contribute (...) by intensifying the (...) international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks', which also addresses the economic issues mentioned earlier.

Our arguments in favour of CCB therefore rely not only on economic considerations, but also on a political narrative supporting an open and free Internet – similar to the strategy developed by the EU. However, to help foster the conditions for a new generation of liberal democracies to appear, these institutions now need to act on their promises and promote access to Internet governance discussions for all stakeholders in developing countries, at the governmental, corporate and societal levels.

The prospective gains for donor countries go beyond the political realm. A focus on cyber security in the development programmes of partner nations will also have positive externalities in terms of international norms that can lead to higher levels of cyber security. The Internet has no borders (yet), so achieving greater security in partner countries will yield cyber security results in donor countries as well. Further, it will help to curtail the growth of cyber-theft, already a major cause of risks for governments and private companies alike.

1.3 Enhancing security among donor and partner countries through coalitions of like-minded states

In a study for the OECD, it was noted that 'Vulnerabilities in software developed in one country and installed in a second can be exploited remotely from a third' (OECD/IFP, 2011). Cyberspace ignores international borders and allows anyone anywhere to attack anyone anywhere else. A compromised device (computer, mobile, wearable device) in, say, Malaysia (or Germany, or Kenya...) can be used to attack a computer in Washington DC, with the true attacker remaining hidden. Cybercriminal gangs (like the legendary Nigerian 419-scammers) can wage international campaigns that know no borders, while avoiding prosecution because their own governments lack the necessary resources. Attackers aiming at more lucrative targets in the governments and private sector of the industrialized world might first seek to compromise partners in the developing world. The potential list is unending, but the point is simple: mitigating against such cyber-risks often requires governments in the developing world to have two principal capabilities. Firstly, well-developed national standards for information assurance purposes, with legal requirements on specific critical infrastructure to take basic minimal precautions, such as the use of basic cyber security products or similar. Secondly, the ability to respond operationally (assisted by CERT or similar organizations) to international requests for assistance in dealing with cyber security issues, both from the security services and the wider community itself.

Neither of these capabilities can be developed in a vacuum: they are influenced and formed by various interests, many of which show breaks along ideological and political lines. There are significant differences between how the 'West' in general sees the Internet, and how countries such as Russia and China see it. What is often agreed upon at

a technical/operational level gets abstracted into 'norms' at the policy level.

There have been repeated attempts to formulate global norms on the rights and responsibilities of states as regards cyberspace, such as the recent push for peacetime international rules of the road under discussion in the UN Group of Government Experts (UN GGE) and within regional forums such as the OSCE and ASEAN. They are also very much a topic of bilateral discussion, as seen in April 2015 when a factsheet released by the White House on US–Japan cooperation affirmed:

'States should uphold additional, voluntary norms of State behavior in cyberspace during peacetime, [...] States should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public [...] the United States and Japan commit to continued discussions to identify specific peacetime cyber norms, noting that wide affirmation among States would contribute to international stability in cyberspace.' (White House, 2015)

However, significant differences remain between liberal democratic countries and less democratic governments around the world. While previously these discussions (such as within the UN Group of Government Experts) were seen as being similar to nuclear non-proliferation discussions – i.e. of interest only to a small elite – the 'militarization' of cyberspace has not stopped at the developing world, with over 130 countries currently developing military cyber-programmes. This has been respected in these discussion forums, which have been greatly expanded to include actors from the developing world. The discussion has become a global one, with greatly differing 'sides' to the narrative – and many 'swing votes' to gather.

The norm development process can occur along two different lines – 'universal norms' that will be binding for all, or a 'like-minded' group of states that seeks to pursue a deeper level of cooperation and enforcement of agreed norms. While the first is the preferred option, the second seems the more likely outcome – at least in the short term.

First option: universal norms

Roger Hurwitz (2014) argues, 'States have agreed on the need for norms as a means to restrain disruptive behaviors in cyberspace and their negative impact on international security'. However, as he also points out, cyberspace has inner differences with the offline world and there is a need to craft new norms to fit those differences. The first round of such norms could include the duty to assist international investigation, the duty to prevent attacks emanating from a state's territory and restrict the recruitment and use of third parties (proxies, mercenaries) to commit wrongful acts.

Those norms would curtail the abilities of non-state actors to commit cyber-attacks, and states would be in charge of crafting and enforcing them on a territorial basis. That is the observation of the (OECD, 2012): 'International co-operation and the need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries are (...) key objectives'.

There are two problems about this ideal view of states agreeing on universal norms. First, it ignores corporate and civil society actors, whose incentives might differ from those of states, notably on issues of security and national security. Second, enforcing norms rejected by the private sector and civil society will be harder, precisely because these stakeholders stand to gain so much from a free and open Internet. This explains why many of the cyber security frameworks in the USA have been developed in partnership with the private sector, such as National Institute of Standards and Technology's (NIST) framework for cyber security (NIST, 2014).

The second issue with state-centric vision of norm-building is that states might not be able to reach such agreements (Goldsmith, 2012). Indeed, there is a lack of mutual interest for states to engage in this kind of norm-building. Firstly, because fundamental asymmetry of offensive cyber capabilities and vulnerabilities mean that different states face different levels of incentives for engaging in norm-building processes, and the incentives of each state are hard to read. Secondly, a lack of clear definitions of the boundaries between sectors (such as cyber-attack and cyber-exploitation) are constantly shifting, so it is unclear how states could agree on them before negotiating on cyber norms.

Moreover, states tend to employ dual standards in evaluating threats and activities, according to their origin a 'threat' or 'activity' in a partner country is evaluated differently from one perceived to originate in a country with which the diplomatic ties are less firm.

Even less likely is going beyond norms to actual treaties – like those defined by arms treaties – due to the obvious dual-use nature of virtually everything in cyberspace, as well as the impossibility of monitoring any agreement. The 'absence of a dependable verification regime will kill a security treaty – even if other hurdles to cooperation (...) are overcome' (Goldsmith, 2012). This question of enforcement is paramount, precisely because cyber weapons are fundamentally different from other kinds of weapons.

Until those issues are acknowledged and overcome, we hold, states should try to build norms not through globally-inclusive coalitions but through a more focused coalition of like-minded states.

Second option: enforcement through a coalition of like-minded states

Assuming that only a group of like-minded states will, initially, abide by the entire set of norms, Jack Goldsmith argues that 'all States should be subject to at least some of them' and that 'other States will come to accept and observe these norms as a consequence of persuasion, confidence-building measures, incentives or sanctions employed by the like-minded States'. The idea is that this coalition of like-minded states, upon reaching a critical mass, will be able to spread the agreed-upon norms through persuasive or non-persuasive international engagement.

The UK's Cyber Security Strategy fully recognizes the need for such regional measures. Its objective 3 – an 'open, vibrant and stable cyberspace' – includes the need to encourage 'international and regional organisations to support capacity building'. The goal is to develop models for international law within the Commonwealth, support technical training with the ITU and engage the Council of Europe or the OSCE in protecting freedom of expression online. This strategy integrates the full range of available means for norm-building, from legal and binding agreements such as international law to non-legal and non-binding confidence-building measures. This shows that our two options are not incompatible – indeed, to spur their effect, states should be pursuing a mixed strategy.

CCB projects, through engagement with all the relevant stakeholders, present a formidable opportunity for donor countries to use their soft power. They should be one of the key programmes used for spreading the norms of like-minded states to partner countries.

Bilateral development and the role of security services and infrastructure programmes

Beyond relatively abstract deliberations on norms, the technical and political reality is that CCB programmes can also have very practical application for the security interests of donor nations. Successful CCB programmes can lead to further cooperation between the military and security services of both sides – beyond the scope of what would normally be called CCB, and more in line with 'mil-mil' or intelligence sharing.

As repeatedly mentioned in our interviews (see Box 3 and Box 4 below), CCB activities are an opportunity for cyber-incident responders to create a global network of relations which in turn can foster cooperation between the agencies where they work. Engaging early in CCB activities will allow donor countries to create a similar security environment in partner countries. This similarity in the structures of security services will promote more efficient cooperation: it will be easier for an incident response team in the UK that detects a cyber-attack emanating from Ghana to tackle this attack if the structure of the incident response team in Accra is similar to their own. That being said, however, a donor

nation might receive operational benefits of cooperation from a partner nation even without the latter knowing it.

A recurrent story in the Western media has concerned how China is 'taking over the Internet in Africa' – largely by installing subsidized Chinese Huawei and ZTE routers in key Internet backbone locations. While some of these activities are understandable market moves as part of an 'African telco gold rush', this has not halted speculations at to other benefits China might derive from having such a controlling position on the physical layer of the African Internet.

Although this aspect is partially unproven, it should be acknowledged that, from a 'hard power' security perspective, there are theoretical advantages to be derived from such a position. CCB, although overwhelmingly a tool of 'soft power', may have repercussions that are directly relevant to harder security concerns.

2. Segmentation of CCB activities

As countries begin developing cyber security strategies, they also begin upping the funds dedicated to Cyber Security Capacity Building (CCB). With this increase has come a growing academic interest in such programmes. Building on the literature of Capacity Building, research efforts have been working on segmenting CCB activities across several sectors. The recent study by the European Union Institute for Security Studies (EUISS, 2014) presents several of those strategies, with an overview of approaches for fostering more efficient CCB activities.

In this section, based on the series of interviews we conducted and the rationale we have provided, we adopt **four** categories to describe the support that donor countries can provide in terms of CCB.

1. **Methodological** support consists of general concepts used for building local capacities, as well as basic research into how CCB works.

2. **Technical** support focuses on training around the CERT/CSIRT structures, the help provided at law-enforcement level and support for community-based instruments.

3. **Infrastructural** support offers examples of successful infrastructural projects.

4. Finally, we examine efficient ways for donor countries to provide **budgetary** support, especially as regards support through international organizations or directly to civil society.

2.1 Methodological support: models and options for partner countries

The concept of 'methodological support' concerns not only delivering models, but includes all policy options available to governments considering CCB activities. As regards the idea of creating overarching methods, two main approaches have been examined and reviewed – one highly descriptive and encompassing, the second more general and focused on security aspects.

Oxford GCSCC: Five dimensions of CCB activities

In early 2015, the Global Cyber Security Capacity Centre at Oxford released the first version of its framework, the Cyber Security Capability

Maturity Model (CMM).[4] It aims at increasing the scale and effectiveness of cyber security capacity building, measuring those capacities with five levels of advancement (start-up, formative, established, strategic and dynamic) along five dimensions:

- devising cyber policy and strategy
- encouraging responsible cyber culture within society
- building cyber skills into the workforce and leadership
- creating effective legal and regulatory frameworks
- controlling risks through organization, standards and technology

Each of these five dimensions, with their subcategories, and their respective 'maturity' (level of sophistication) has been broken down into 225 individual descriptions. This level of detail is both an advantage and a risk: at times the descriptive text seems overly simplistic, especially at higher levels of 'maturity'.

Only the first dimension – 'devising cyber policy and strategy' – seems to concentrate on actual cyber security, with some strong support from the fourth dimension (legal frameworks). Overall, of the 20-odd subcategories (one sub-category without content is presumably a work in progress) only some six to eight have a direct bearing on traditional understandings of national cyber security. The others concentrate on other important societal aspects clearly relevant for issues of national security, such as 'mind-sets' and education.

Establishing a maturity model for an issue as complex as national cyber security capabilities will always be a difficult and perhaps also unachievable task. While ideas of a 'capability model' have been used in the last decade in some types of management consulting (including in evaluating software development), they are less often applied to such complex and non-linear concepts as national strategies, or capabilities. The primary challenge will always be the perception of an overtly normative approach – applying and promoting a certain set of values or standards, and putting them in qualitative ranking to each other (with some 'less developed', others 'more developed'.) On the other hand, it can be argued that, since all approaches are at least somewhat normative, this may be a rather moot point. In this case, however, it is important that the underlying evaluations/descriptions be as detailed as possible. As the current version of the GCSCC Model is

4 Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/gcscc-cyber-security-capability-maturity-model-cmm [Accessed 8 June 2015].

still partially a draft, future versions may well address these open questions.

EUISS: Four pillars of CCB activities

The EUISS approach (2014) focuses much more on actual security issues in CCB. Taking the standard cyber security incident response model as the point of departure,[5] the EUISS transposes this industry standard approach to the security/development nexus. The EUISS arranges CCB into four stages of concrete security objectives and four pillars of actions aimed at developing local cyber security capability. The concrete security objectives are:

- **Prevention**: Addressing man-made risks associated with cyberspace. This includes investigating the causes of cybercrime, raising awareness on cyber security risks, addressing vulnerabilities and coordinating national policies.

- **Protection**: Collaboration between private and public actors, aimed at reducing the impact of cyber-accidents. This includes developing appropriate CERT structures, legislation, standards, risk assessments, and joint exercises, to promote efficient and well-governed collaboration.

- **Pursuit**: Relying on responsibility assessment for the liability and potential sanctions following cyber-attacks: especially crucial in criminal cases. This includes having frameworks in place for information sharing, understanding the threat and ensuring the cooperation of various authorities with international legal instruments.

- **Response**: Minimizing and managing the negative consequences of a cyber-attack, relying heavily on a CERT/CSIRT and contact points available round the clock.

Common to all four objectives is the development of **cyber resilience.** As noted by Elena Kvochko (EUISS, 2014), 'the risk from major cyber events could significantly slow the pace of technological innovation over the coming decade' and 'a backlash against digitisation could leave as much as US$3.06 trillion of (...) value unrealised'. From that perspective, traditional approaches to cyber security are *ex post;* they fail to involve businesses, require talent that is scarce and expensive, and rely on technological innovations – leaving customers and employees as the vulnerable weakest links.

5 See for instance http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (p.21) [Accessed: 10 June 2015].

The EUISS authors advocate 'cyber resilience', without indicating how it could look (or does look) in practice. Firstly, they mention that risk markets (i.e. insurance products) seem to offer an opportunity for evaluating and ensuring against the risk of cyber-attacks. The mere existence of a risk market offers business opportunities to those who are better able to evaluate those risks, which is a first step before being able to offer the right set of insurance contracts against them. However, the EUISS study fails to consider that it has been the consistent failure of those markets to get established that has prompted a 'creeping' approach to mandating critical infrastructure protection (CIP) measures. Secondly, the authors advocate research on **embedding security** into the early stages of software development. While this seems to offer promising avenues for heightening the overall reliability of security systems (and is increasingly part of CCB programmes), the problem is the level of specificity – for instance, CERTs teaching each other about how to securely code SIEMs and other technical systems will not address the wider and pervasive problems of poor security in the industry.

The four EUISS pillars for building national and regional capacities are:

- **Concepts and strategies**: Determining what needs to be protected and how, and protecting the economic gains of a connected business environment seem to be a 'key driver for cyber security efforts', but sovereignty or particular ethical and cultural values might also broaden the scope of what needs to be protected.

- **Laws and policies**: Developing normative frameworks is itself part of a CCB exercise, as well as legal capacity-building activities. Internationally endorsed principles such as the rule of law can contribute the reshaping of cyberspace to foster human rights, good governance (understood as 'law-making based on the participation of all potential recipient and openness') and cyber security (EUISS, 2014). The legal dimension of cyber security activities has focused especially on

    - data protection and human rights (based on the European Convention of Human Rights and UN discussions on the right to privacy in the digital age),
    - substantive criminal law (based on the Budapest Convention)
    - international binding or non-binding normative framework for state behaviour (based on Article 51 of the UN Charter and international humanitarian law).

- **Organization**: CCB includes the development of the structures corresponding to a national cyber security strategy and other structures as CERTs responsible for coordinating national cy-

bersecurity among all involved actors (intelligence agencies, regulators, law enforcement agencies and defence ministries)

- **Implementation**: CCB programmes require budget, skills (developed through training, education and awareness), technological equipment (physical infrastructure) as well as coordination (through public–private partnerships for example, or information-sharing and analysis centres that act as information clearing houses)

Further methodological support for national cyber security

The models described above are attempts to deliver CCB programmes, or to evaluate the overall state of a country's national cyber security status. For governmental organizations considering both how to target and evaluate the impact of such a strategy, these models can be helpful. However, it is important to note that there are other methodologies that have been used to provide input into many national cyber security strategies, some with considerable influence. Both the NATO CCD COE 'National Cyber Security Framework Manual' and the ITU 'National Cyber Security Guide' are documents that have been used by developing countries to help formulate and plan their own individual national approaches to cyber security. As noted in section 1.3 above, the competition of political ideology also translates into differing strategic and operational approaches at the norms level, and the NATO and the ITU documents are emblematic of the differing general approaches.

The differences are even starker as regards international agreements with strong practical application. For instance, the Budapest Convention on Cyber Crime is by far the most widely accepted international agreement with cyber security implications in current use. It provides effective guidelines on how to set up law enforcement and criminal prosecution systems; therefore, countries which adhere to the Convention are much more likely to cooperate effectively with each other on cyber security incidents. However, several countries – most importantly Russia and China, but also Brazil and India and others – have rejected the Budapest Convention. Russia and China have sought to provide a counter-document with the International Code of Conduct on Information Security, and have pursued an international strategy dedicated to its promotion. These documents are very different – also in scope and application – but both have the same aim: to convince signatories to adhere to a particular vision of national cyber security. The methodological relevance of these documents cannot be ignored: they sometimes represent the most important guides for developing countries.

BOX 1: The National Cyber Security Framework Manual

These objectives and areas are all captured in the NATO CCD COE–sponsored *National Cyber Security Framework Manual (2012)*, where Klimburg and others argue that the development of national cyber security programmes doctrines need to take into consideration five 'mandates' that account for various differing approaches (see below). These five mandates all have roles and responsibilities derived from the industry-standard Cyber Security Response Model (pro-action, prevention, preparation, response, recovery, and aftercare/follow-up) The development of these strategies should centre around various 'dimensions' – Whole-of-Government 'coordination' on mandates, Whole-of-System 'cooperation' on international issues in a like-to-like context, and a Whole-of-Nation 'collaboration' approach aimed at convincing local (national) actors to engage in activities conducive to supporting national cyber security. While every governmental system has its own political realities to address, each will have various dilemmas it needs to solve, and that will depend on specific local conditions.

National Cyber Security (NCS) Defined	'The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'
The 5 Mandates Different interpretations of NCS & common activities	– Military Cyber – Counter Cyber Crime – Intelligence and Counter-Intelligence – Critical Infrastructure Protection and National Crisis Management – Cyber Diplomacy and Internet Governance + 3 'Cross Mandates': coordination, information exchange and data protection, research & development and education
The 3 Dimensions Different stakeholder groups in NCS	– Governmental (central, state, local) – 'coordination' – National (CIP/contactors, security companies, civil society) – 'co-operation' – International (legal, political and industry frameworks) – 'collaboration'
The 5 Dilemmas Balancing the cost and benefits of NCS	– Stimulate the Economy vs. Improve National Security – Infrastructure Modernisation vs. Critical Infrastructure Protection – Private Sector vs. Public Sector – Data Protection vs. Information Sharing – Freedom of Expression vs. Political Stability

(source: *National Cyber Security Framework Manual*, 2012)

BOX 2: The Council of Europe Convention on Cybercrime (Budapest Convention)

The Council of Europe Convention on cybercrime (the Budapest Convention) is the only widespread convention to address definitions and practices in dealing with cybercrime. Opened for signature in 2001, it entered into force in 2004 after ratification by five countries including three member-states of the Council of Europe. It has since been ratified by 46 countries, and signed but not ratified by an additional eight.

The Budapest Convention is not a treaty, but a methodological framework for help in designing mutually compatible legislation on cybercrime. It defines appropriate measures for substantive criminal law to be taken for offences against the confidentiality, integrity and availability of computer data and systems, for computer- and content-related offences as well as for infringements of copyrights and related rights. It also defines the procedural frameworks needed for dealing with those offences (common provisions, preservation of stored data, production orders, search and seizure, real-time collection of data) and tries to tackle jurisdictional issues. Finally, it sets a framework for international cooperation including mutual assistance and a round the clock point of contact for immediate assistance in investigating, proceedings or collecting evidence.

As such, it is a truly unique document which can go far in helping governments find a common basis on which to communicate on cybercrime related issues. As it is very difficult for countries to be able to engage in any kind of cooperation on this issue without having acceded to the Convention – or to implement its measures without being a signatory – its importance as a methodological tool for CCB cannot be overstated.

2.2 Technical support for Computer Emergency Response Team (CERT), law enforcement, Internet Service Providers (ISPs) and community-based instruments

Support for CERTs/CSIRTs

CERT/CSIRT structures are vital operational components of cyber security, and various documents have been prepared to help partner countries develop their own CERT/CSIRTs. After publishing, as early as 2006, a step-by-step approach on how to set up a CSIRT (ENISA, 2006), the European Union Agency for Network and Information Security (ENISA) memorably described CSIRTs as ‘a fire brigade (...) the only ones which can react when security incidents occur’ (ENISA, 2008).

This description is too modest (highlighting only the life-saving functions of CERTs): more than just a 'fire brigade', CERTs are akin to insurance, building-code supervisors, and law enforcement investigators.

However, if early approaches focused on sectoral CSIRTs, national CSIRTs have since received greater attention as states developed their understanding and research on cyber security, Critical Information Infrastructure Protection (CIIP), and increasingly on national crisis management issues.

BOX 3: From an interview with Koichiro Komiyama, Deputy Director of Global Coordination Division and Manager of Enterprise Support Group of the JPCERT/CC, and Member of the Board of Directors of Forum of Incident Response and Security Teams (FIRST)

The JPCERT/CC is a non-profit NGO, but its budget is mostly covered by the Japanese Ministry of Economy, Trade and Industry (METI). It is responsible for protecting Japanese Internet users, including infrastructures within the national CIP framework. Their work in cyber capacity building has focused on **CSIRT establishment** at the **national** and **regional** levels, as well as **workshops on secure coding**.

In terms of **CSIRT establishment**, JPCERT/CC are seeking to build **national** organizations and have been working with FIRST to draft a model for CCB activities by CSIRTs that they will then enrich with their experience on the ground. They recognize that their work is facilitated by the development of **regional** CSIRTs that organize and promote the collaboration at their own level. In the absence of regional CSIRTs in either the Pacific or African regions, they are working with individual countries like Tanzania and Fiji to foster their leadership in the creation and development of regional entities.

The strategy for their training is organized in three areas: **why** is it in the interest of partner countries to care about CSIRTs and cyber security? **what** is a CSIRT? (with examples of CSIRTs that have proven useful) and **how** to build a CSIRT, including a focus on operational issues.

Occasional **workshops** are arranged, especially on secure coding. This is a dual-use measure that both increases the local pool of technical skills and is also a way of introducing local researchers to the global community, to facilitate trust and create a network of personal relations in the field of cyber security.

The debate on what constitutes a 'national' CERT can be a vexing question. The OSCE – within the context of developing the IWG 1039 norm package – spent significant amounts of time on this issue, and community-based organizations such as FIRST have also started to try to define the difference between government-mandated 'national' CERTs

and others. There are significant differences in the capabilities of CERTs: they can range from NOC/SOC configurations with ability to 'pull the plug' if needed, to purely advisory components with limited operational roles. Some 'national' CERTs are tasked only with defending government networks (if allowed: many governmental CERTs cannot override decisions taken by sectoral CERTs) while some have a truly national role, directly helping to protect their countries' critical infrastructure. The only key component that all 'national' CERTs must have is the ability to serve as an authorized point of contact for technical issues – for major incidents, but much more likely for the day-to-day fight against cybercrime. This category includes much of what may be construed as state-supported cyber-espionage.

BOX 4: From an interview with Eunju Pak (Deputy Researcher at the KrCERT/CC and Senior Research Associate at the Korea Information Security Agency)

The KrCERT/CC is under the authority of the Korean Internet & Security Agency, in turn under the Korean Ministry of Science, ICT and Future Planning – from which their funding comes exclusively. The CCB team belongs to the Incident Response Division, and it is their duty under various international cooperation programmes to engage in CCB, in order to establish **reliable relationships** among CSIRTs in the Asia-Pacific region.

They achieve those goals mainly through the five-day training course at APISC (Asia Pacific Information Security Center) based on TRANSITS I (Training of Network Security Incident Team Staff), a regular training course developed by the TERENA (Trans-European Research and Education Networking Association) for establishing and operating a CSIRT. This TRANSITS course covers organizational, technical, operational and legal issues, in two steps:

1. TRANSITS-I[6] is 'aimed at new or potential CSIRT personnel who wish to gain a good grounding in the main aspects of working in an incident handling and response team.'
2. TRANSITS-II[7] is 'aimed at more experienced personnel working for established CSIRTs. It provides in-depth study of key areas in incident handling and response operations, training in how to improve communications with constituents, along with practical exercises.

6 https://www.terena.org/activities/transits/transits-i/
7 https://www.terena.org/activities/transits/transits-ii/

Support for law enforcement

Increasingly CERT/CSIRT issues are overlapping with wider cases of law enforcement (LE) cooperation. Where technical cooperation programmes are offered by a donor nation, they often address issues such as computer and network forensics or procedures for engaging in MLAT (Mutual Legal Assistance Treaties) – all critical issues when dealing with cybercrime. The reason for this overlap between LE and CERT activities is probably a practical one: national CERT activities are often closely connected to those of LE.

In the fight against cybercrime (ENISA, 2012), the CERTs and LE are 'paramount and indispensable players', hence the goal of improving the 'capability of CERTs (...) to address the network and information security (NIS) aspects of cybercrime'. The ENISA report concludes that it is 'undoubtedly important for [LE] teams to know that they can count on the expertise of a CERT team for assistance in handling certain cases'.

That being said, organizing specific LE-related activities is often quite politically contentious, and can involve a range of programmes and procedures. CERTs activities represent a practical and less-contentious method for donor countries to engage with the security services of various countries. The most obvious reason for CERTs to be engaged in the space is simply 'community building': among first responders, there is a strong belief in the importance of informal networks to facilitate not only information sharing, but also incident response. Addressing the needs of partner nations is therefore seen as a crucial step in building mutual trust within the all-important community networks.

Support to community-based instruments and ISPs

Given sufficient technical capabilities, the operational activities of CERTs often require live feeds about cyber activities, important primarily for identifying what is 'bad' on the Internet, and further forensic activities that can be useful in the usual CERT context but also for LE purposes. Those instruments are described extensively in ENISA (2011), where the goal was to 'investigate ways in which CERTs (...) proactively detect incidents concerning their constituencies'. Proactive detection of incidents is there defined as 'the process of discovery of malicious activity in a CERT's constituency through internal monitoring tools or external services (...) before the affected constituents become aware of the problem'. Those external services are almost entirely community-based resources.

Such resources may be public, closed or commercial, but in all cases they can be shared by multiple cyber security responders in a largely apolitical way (some may require 'some form of vetting of the recipient' of the feed, or a subscription fee). Besides the private sector, many of these instruments are developed and maintained at the level of civil

society: the ENISA report notes that they are 'run by various security organisations, projects, vendors, universities, CERTs or non-profit initiatives, or even enthusiastic individuals'.

Examples of such businesses include the Shadowserver Foundation,[8] an organization of 'volunteer security professionals around the world [...] seeking to provide timely and relevant information to the security community at large', and Spamhouse, a long-established project that provides up-to-date list of 'bad Internet domains' and spam groups that other organizations can then block for malicious traffic. The community is even engaged in building physical infrastructure: Packet Clearing House, for instance, builds and manages various Internet eXchange Points around the world (IXPs). (see Box 5)

However, as mentioned in the interview (Box 5), the number of CERTs in partner countries with technical capabilities for exploiting such feeds is limited. Therefore, the development of localized community-based instruments, albeit crucial for a sustainable healthy cyberspace constituency, might require initial CCB activities with technical training of CERT and LE teams. That makes it more meaningful to first support the work of existing community-based instruments, and, where necessary, their expansion to include further geographic areas (for instance, in sub-Saharan Africa). Localized (partner-country) initiatives should be supported wherever possible, but in the short term it is essential to ensure that the partner CERTs and similar organizations are in a position to exploit the resources available.

2.3 Infrastructural support: development of economic infrastructure

Physical infrastructures are crucial for economic development. As we already mentioned, a 10% increase in broadband penetration is associated with an additional 1.38% increase in GDP (IC4D, 2009). Moreover, countries with higher broadband penetration typically experience 0.023–0.026% in GDP growth for each 1% growth in broadband penetration; by contrast, for countries with low broadband penetration, the contribution to GDP growth ranges between 0.008 and 0.021% (ITU, 2012).

Physical infrastructures also increase the demand for technical skills. Therefore infrastructural support must be coupled with activities aimed at increasing the local supply of technical skills — such as training activities.

Different models for infrastructural support

The World Economic Forum (WEF, 2015) has provided a list of operating models that emerging markets are experimenting with, and a list of

8 https://www.shadowserver.org/wiki/

factors which can help in determining which are appropriate in various contexts:

- **Infrastructure sharing**: Reduces the profitability gap and can be done at multiple levels. For instance, tower sharing is common in India; and passive network-sharing agreements are common in Bangladesh after the government mandated the signing of such agreements.

- **Government subsidies for rural rollouts**: Compatible with 'last mile' competition between operators. The WEF reports mixed results, with 64 national funds established for universal service but very few of them actually making use of their full budget.

- **Rural wholesale network**: Funded partially or fully by governments, then provided without discrimination to mobile operators, a level playing field for competition at the retail level. WEF reports that governments have not been good network operators and that these networks may 'hamper innovation if not actual coverage'.

- **Private investment** and **other innovative approaches**: Private firms like Facebook or Google have incentives for developing coverage in partner countries if they expect to extract economic benefits from the newly covered populations. Initiatives like Internet.org (Facebook) or Project Loon (Google) have been developed precisely to fill in this gap. However, it is unclear whether the services provided are backed up by sufficient local capabilities so that partner countries are sustainably connected to an open and secure Internet.

In all these cases, a crucial decision has to be made by local governments. The WEF report lists potential priorities according to environment (rural/urban) and wealth (moderate or low GDP per capita) criteria. Beyond choosing a model for extending coverage, governments also have to encourage the use of infrastructure to trigger the associated economic benefits.

The role of local governments

Local governments can play three main roles (Dalberg, 2013):

- **Government as a visionary** fostering good leadership can define a national **strategy** for the Internet and ICT use. This sends an important signal to stakeholders and is also a practical way to align a diverse set of national actors.

- **Government as a catalyst** of good governance can create an **environment** within which actors can invest and collaborate

around the use of the Internet. This is a role that no other local actor can take on, with the same level of efficiency.

- **Government as a first adopter** and promoter can make the first use of the Internet's various capabilities. This is crucial to wider national usage and to realization of the **impact** of infrastructural developments.

In the roles mentioned above, results stem from a thriving ecosystem of locally-owned businesses. In that sense, encouraging local ownership may entail economic losses for Western companies but will yield political gains that offset these losses. Local ownership also feeds our other segments, by increasing the demand for local technical personnel and providing the terrain for the implementation of the methodologies mentioned. Local ownership was also an issue mentioned in the interview with JPCERT/CC (see Box 3): since there are no private actors able to capture the economic benefits that would be produced, there are few incentives for partner countries to engage in these projects. ICT is a source of local economic growth not only in Africa; it is also a source of economic growth for multinational companies that are developing in Africa. And the fact that submarine cables are owned by multinational companies generates economic benefits for the owners of the submarine cables, rather than for partner countries.

However, the incentives of both governments and multinational companies can be mixed. To be efficient and sustainable, infrastructural support must be linked to other activities that enhance local usage. Here, training has been used to both supply the skilled labour necessary for the infrastructural project and foster an environment conducive to local usage.

The experience of the NGO PCH is instructive. Two issues that they typically encounter when seeking to build IXPs are administrative traps and overinvestment. In terms of administrative traps, there is for instance little need for a feasibility study before building an IXP ('you don't do a feasibility study for a street – you just build the street'). In terms of overinvestment, it is important to match the size of the IXP with the needs of the country, because overinvestment lowers the price/performance ratio considerably.

Supply side: synchronizing infrastructural projects with trainings

Infrastructure activities provide occasions for organize training activities in order to promote an increase in supply and demand for technical skills. South Korea's KISA, the mother organization of KrCERT/CC, has been actively involved in CCB activities in Rwanda: after a Korean ISP had been contracted by the Rwandan government to build the infrastructure of a Rwandan CSIRT in 2013/2014, KISA dispatched skilled KrCERT/CC staff to Rwanda to provide training there.

BOX 5: Interview with Bill Woodcock, Executive Director of Packet Clearing House

Packet Clearing House (PCH) is a global NGO funded by businesses and governments with the purpose of addressing large-scale problems that affect the growth of the Internet (scalability, economic problems, lack of trust and regulatory issues that involve a lack of understanding between the public sector and private companies). PCH focuses on areas where growth is low, with the objective of bringing those areas up to the global Internet average of doubling in size every 10.5 months. Such unequal growth exacerbates the digital divide and harms the future business prospects of Internet companies that rely on the continuing expansion of the Internet. PCH works in four main areas:

1. **Internet Exchange Points (IXPs)**: IXPs are the 'factories that produce Internet bandwidth' and constrain the supply side of Internet growth. All the connected populations in the world consume bandwidth, which, at a national aggregate, can be considered as an export/import question: is a country a net exporter or net importer of bandwidth? The world's largest net exporter of Internet bandwidth is the Netherlands, whereas the 43% of countries without IXPs are 100% importers. In economic terms, 90% of IXPs cost between $4k and $40k, and almost all of them return that investment within less than a week. After the Edward Snowden affair, national security and privacy arguments are also being used to rationalize the construction of IXPs, as they avoid the necessity of routing Internet traffic through another country where different legal and regulatory systems prevail.
2. **The core of the Domain Name System (DNS)**: the DNS is a critical infrastructure that allows things to be found on the Internet. PCH operates the world's largest authoritative DNS service platform, supporting operators of root and top-level domains as well as providing them with training and logistical support. PCH's anycast platform is typically more resilient to Distributed Denial of Service (DDoS) than other alternatives. In addition, PCH operates the only FIPS 140-2 Level 4 DNSSEC signing platform other than the one that ICANN (Internet Corporation for Assigned Names and Numbers) maintains for the root zone.
3. **Regulatory and policy issues**: there are areas where the most fundamental problems are regulatory or political, and PCH engages directly with governments on longer-term and larger-scale economic development and national and regional infrastructure planning projects. The main issue around building IXPs is usually that those stakeholders that have an interest in the status quo may be very powerful locally, including in regulatory bodies. The roles of governments with respect to ccTLD administration and multi-stakeholder Internet governance are also topics on which PCH is frequently engaged by national governments.
4. **Cybersecurity coordination**: PCH operates a CERT that does not engage in digital forensics or in finding malware, but in helping cyber security practitioners to locate and connect with the right parties to resolve an issue. They are sometimes asked to do a first-pass of forensics to gather more information about a situation or issue that arises for teams with little technical ability. PCH is also the secretariat for INOC-DBA, the lower tier of the two-tier Internet emergency coordination system.

What building an IXP involves

The global directory of IXPs is made available by PCH online.[9] IXP formation is typically **funded** by voluntary donations by their participants, by PCH, or by donor organizations like the World Bank. They are not difficult to build, from a business or from an economic perspective. However, they often encounter problems with incumbent monopolies that attempt to block their formation, fearing competition from the new market entrants that IXPs enable. This situation is further complicated by the fact that some regulatory agencies are not *de facto* independent from those monopolies, which are sometimes publicly owned. Before local Internet Service Providers (ISPs) get used to working with each other and collaboratively producing the bandwidth that they use, they are often aggressive competitors: this can make the initial formation of IXPs difficult because ISPs lack the collegial relationship that characterizes more mature environments. Some countries also encounter **infrastructural issues,** when IXPs are set up but the ISPs lack the fibre to connect to them. Finally, technical training for ISPs is something that PCH has been delivering for over twenty years.

Countries need to build critical scale first in order to take advantage of the impacts of network coverage. We believe that in many of the cases where the economic incentives are not present for donor countries to engage in infrastructural support, careful studies of the potential gains might provide a sufficient basis for becoming involved in such activities. Furthermore, synchronizing infrastructural activities with training activities is one way to foster a personal network of experts that can provide effective response after a serious cyber-attack, in partner or donor countries.

2.4 Budgetary support: comprehensive programmes

The past decade has seen a marked shift within Official Development Assistance (ODA) towards direct budgetary support as a tool for aid. There are two different types of direct budgetary support – 'general' budgetary support, which is completely untied and left to the discretion of the partner government, and 'sectoral'. This analysis is concerned with the applicability of 'sectoral' aid – budgetary support that may be used by the partner government within a specific area only. Here the term 'budgetary support' is used as shorthand for 'comprehensive support initiatives'– governments that engage in such activity tend to support all the previous types of engagements (methodological, technical, infrastructure) besides providing funds directly to partner governments for operational expenses.

In terms of volume, some of the larger budgetary support items will include funds for large-scale infrastructure development – most importantly, supporting the expansion of telecommunication facilities.

[9] https://prefix.pch.net/applications/ixpdir/

These programmes are covered in 2.3 above; the focus here is on budgetary support initiatives that go beyond one-off projects: funding sustained local engagement with partner governments.

As our UK interview partner pointed out, it is important for donor countries to align their CCB efforts with their foreign policy. Using roughly the same segmentation as indicated in this report, the UK provides funding primarily for short-term projects, to be able to keep a certain level of flexibility. This makes it possible to maintain alignment between CCB efforts and foreign policy goals. For longer-term projects, however, it is necessary to work with international organizations.

BOX 6: Interview with Tony Clemson (Head of Cyber Security Capacity Building & Prosperity, Foreign & Commonwealth Office, UK)

The UK's National Cyber Security Strategy received £860m in support for the period 2011 to 2015. Of this budget, the FCO's Cyber Security Capacity Building Programme (CSCBP) represents approximately £2m per year. About one third of the resources of this programme are allocated to tackling cybercrime and capacity building for **LE** and **judicial systems**, as well as for the improvement of **international LE coordination**. About half of their total capacity-building activity is reported as Official Development Assistance.

The CSCBP of the Cyber Policy Department of the Foreign & Commonwealth Office follows rather closely our segmentation of cyber security capacity building activities:

1. **Methodological**: The UK funds **research** through the University of Oxford's Global Cyber Security Capacity Centre. This funding represents approximately 25% (about £0.5m annually) of the capacity building fund.
2. **Technical**: Support is provided to countries to develop their **national strategies**. That is a much broader work and a longer-term investment than other activities, but it is held to assist in building global cyber resilience. The CSCBP has, for example, funded the OAS to help develop the cyber security strategy of Jamaica. Finally, the Programme helps to strengthen national CERTs through FIRST **trainings** – it funds FIRST to develop and deliver training without getting directly involved.
3. **Infrastructure**: Work concerning **critical infrastructure** overseas is conducted with partner organizations that want to build resilience, like the government and businesses of the Kingdom of Saudi Arabia.
4. **Budgetary**: There is a **multiplier effect** in working with international organizations, since capacity is built at both the organizational and the local levels. The UK, for example, works with organizations like OAS or the Commonwealth Telecommunications Organization and the Commonwealth Cybercrime Initiative.

Agility is a crucial aspect of projects because it allows for an alignment with national foreign policy. Projects therefore generally run for less than a year so that they can retain that flexibility. They are in constant dialogue with partners to coordinate international response with the needs and priorities.

Direct budgetary support – operational expenses

As noted, donor governments can (and, most likely, increasingly will) engage in directly sponsoring individual government budget lines, particularly regarding LE, military and SSR-related tasks. Cyber security serves to encourage this trend, as many 'national' CERT functions are maintained in a public–private partnership (PPP) with a local company. For instance, Austria maintains a 'government' and a 'national' CERT: and both are partially supported by the local Internet registry, Nic.at. An arrangement that among OECD countries is often born out of necessity is actually a great boon for partner nations (and their donors): a significant problem for partner countries is not only the ability to attract (and fund) good talent to CERTs and related institutions, but also managing these challenges within the constraints of government guidelines. For instance, it is hard to envision an average sub-Saharan government salary being at all attractive for a local information security professional, who could probably earn up to a multiple of ten times the government rate. If that person is trained up internally, he or she is likely to leave at the earliest opportunity. With a PPP, 'market rates' can be paid for local talent, talent that government salaries find extremely difficult to attract.

While there are currently no known examples of entire CERTs or similar being funded by donor nations, they probably exist – and probably represent a future trend.

BOX 7: Interview with Heli Tiirmaa-Klaar (Head of Cyber Policy Coordination, Conflict Prevention and Security Policy Directorate, Europan External Action Service (EEAS))

Organizationally, after 2011, the EEAS is a rather large organization, with 7,000 people overall. It is managed by the EU High Representative for Foreign Affairs and Security Policy and is reporting to the EU Foreign and Defence ministries. The EEAS cyber policy coordination combines diplomatic and defence issues, mainly concerning cyber-norm development, confidence-building measures, cyber dialogues and dealings with international organizations like the UN, World Summit on the Information Society (WSIS), and NATO CCD COE. They also deal with counterparts within the EU (e.g. DGCONNECT, DGHOME) as well as EU member-states. They work through the Council Working Groups and the horizontal Friends of Presidency Group on Cyber Issues which allows them to work across EU competence areas.

The EEAS structure for Cyber issues includes approximately 10 people within a larger coordination structure of 40 persons, including desk officers.

Why Cyber Capacity Building?

The EEAS engages in CCB mainly for four reasons:

- to prevent threats (security reasons): cyberspace is not a castle and the EEAS wants to make sure that countries around the world are dealing with such issue, to avoid negative externalities (in Africa, for instance, only circa 10 countries currently have cybercrime laws)
- to promote the principles included in the Budapest Convention on addressing cybercrime around the world
- to promote ODA, which is a logical outcome of the diplomatic efforts of the EU and one of its great strengths
- to support the multi-stakeholder model through the side-effects of equipping countries with cyber expertise.

The EEAS is in charge of the political steering of the EU CCB activities, as regards geographical areas and budgeting operations. The focus is global since the EU assistance instruments used for cyber capacity building are of a global nature. There is no formal limitation to any country or region, but the selection process of target countries include a wide variety of elements, such as human rights situation, institutional maturity of the country, willingness to cooperate with the EU etc. However, the EEAS is investigating new initiatives to foster donor coordination, such as the Global Forum on Cyber Expertise.

Cooperation with and through international organizations

In addition to international organizations like the World Bank that directly fund very large-scale projects (e.g., IXP projects, as mentioned in Box 5), we have interviewed international organizations that focus on political coordination of smaller efforts (see Box 8).

BOX 8: Global Forum on Cyber Expertise: a boost to global cyber capacity building (from an interview with Wouter Jurgens, Head of Task Force International Cyber Policies, Ministry of Foreign Affairs, Netherlands)

Capacity-building is gaining prominence as countries and companies become more dependent on the cyber world. In this context, the Global Forum on Cyber Expertise (GFCE) was launched on 16 April 2015 by the Netherlands and 42 partners. Through a flexible action-oriented forum dedicated to meeting the challenges facing various sectors, the goal is to share knowledge and expertise without duplicating existing efforts, seize the economic opportunities that cyberspace offers, and complement the efforts of other member and non-member countries.

Funding for the GFCE Secretariat now comes from the Dutch government (between €2m and €2.5m). In addition, the Dutch government provides funding for the Dutch GFCE initiatives; members are expected to contribute to their own CCB initiatives. The GFCE is one of the most concrete outcomes of the Global Conference on Cyberspace (GCCS) 2015 and the Dutch government is highly committed and optimistic to see it develop into an international forum that will strengthen cyber security capacity and expertise globally.

The GFCE members have started working on four priorities:

1. **Making an inventory of current efforts in CCB**. Through an agreement with Oxford University to include GFCE in its portal[10] and examine efforts in areas and regions throughout the world, the GFCE aims to make information available to its members and the public, providing a convenient overview of CCB initiatives worldwide.
2. **Providing an umbrella framework and organization for CCB initiatives**. For example, when a GFCE member mentions a certain issue (related to raising awareness, building a CSIRT, responsible disclosures, cybercrime etc.), the Forum aims to provide a platform able to connect with other members already working on the issue so they can help each other achieve a safer cyber domain. GFCE members have already announced the launch of 10 partnered CCB initiatives, building on previous work and on their own expertise. In the first group of initiatives, the focus is mainly on cyber security: Norway, OAS and the UK are now working on a Global Cyber Security Capacity Model to assess capacity on a national model; a cyber awareness initiative for governments, business communities and citizens has been set up by the Netherlands and Senegal; Symantec, the USA and the African Union Commission have started work on a report on policy frameworks around cyber security and cybercrime in Africa.
3. **Organizing an annual high-level discussion** with all GFCE members to discuss trends, initiatives and exchange thoughts and best practices, as well as assess current activities. Those discussions will typically be arranged on the margins of the GCCS (the next is scheduled for Mexico in 2017). Before 2017, one will be arranged in 2016, but the venue is not yet decided.
4. **The GFCE will be supported by an administrative unit** (located in The Hague) to be funded by the Netherlands for the time being. The Dutch hope that, in the future, other GFCE members will also take turns in supporting (financially or in kind) this administrative unit, since the initiative is global.

10 https://www.sbs.ox.ac.uk/cyber security-capacity/explore/gfce

Funding for participation in Internet governance

A key aspect of the budgetary support that donor countries can provide concerns help in addressing the three resource constraints for true engagement in the field of Internet governance (Klimburg, 2006):

1. 'Greatly increasing travel requirements for those wishing to be involved in Internet governance.' Physical meetings and conferences are held all around the world, and the travel costs are a serious constraint – in practice, diplomats and businessmen crowd these meetings, instead of academics or volunteers.

2. 'Increasing knowledge demands that are being placed on participants.' Participants are expected to be familiar with a wide array of issues, from technical issues related to the IETF to ICANN documents to diplomatic, security and privacy issues. Educating specialists of one field in several other fields is costly, in both time and money.

3. 'Access to esoteric information (...) is becoming a valued currency.' With 'international cyber security' at the centre of attention, governments and businesses can use information not accessible to civil society participants. If states can rely on confidential information and businesses on corporate data, it is increasingly difficult for people representing civil society to build a rational and data-driven opinion.

Funding for travels, funding for education and funding for community-based instruments producing open data are therefore key constraints. Several international organizations engage in such budgetary support targeting civil society, such as ICANN's Development and Public Responsibility Department (see Box 9), that aims to 'create shared value in the global Internet ecosystem and amongst current and future community members.'[11]

11 https://www.icann.org/news/blog/public-responsibility-a-year-in-review

Box 9: Interview with Jeffrey Dunn, Supporting Education and Academic Outreach Track at the Development and Public Responsibility Department (DPRD), ICANN

The Supporting Education and Academic Outreach Track manages relations with universities, schools, and non-profit bodies in order to organize events and help them understand what ICANN does. It is a young division of the DPRD (one of the four tracks), and currently involves one of the five persons working in the Department. The division supports on-the-ground activities with VPs or global leaders in the organization of events by providing funding, materials or contacts – such as an upcoming event on cyber security and diplomacy with the Permanent Mission of Egypt in New York prior to WSIS. 50 to 60 such events are supported each year, and that does not include the work done by regional teams. The aim is to be as little top–down as possible, leaving it to the community in question to decide the best practices.

ICANN has several programmes focused on outreach, so that members of the public can understand better how ICANN works and are better able to engage in the global field of Internet governance.

- The **Online Learning Platform** is currently under renovation to allow the community an easier way to create, monitor, and update their own courses. The goal is to offer in-depth learning resources to current and future members of the ICANN community. Courses are provided, such as beginner's guides and documentation, to foster understanding of the DNS system. All these activities are considered as 'CCB' because people learn about and engage with Internet governance. The platform include 10,000 active monthly learners; the intention is to reach even more people by providing classes in additional languages beyond the six official UN languages.
- ICANN also organize in person events through the **Fellowship programme**. For this programme, there is no age restriction; funding is provided to a few dozen people who lack the resources to attend ICANN meetings. This kind of budgetary support (limited to three participations per individual) is closely tied to economic and geographical conditions.
- The **NextGen@ICANN initiative** focuses on persons aged 18 to 30. The organization brings in a small number of people to ICANN meetings and works with them in concert with their current occupations (usually as students).

3. CCB and Official Development Assistance

CCB is an effort that benefits both donor and partner countries. For the donor countries, the benefits involve security and political gains; for the partner countries, an enabled business environment that can spur economies to develop in a balanced and sustainable way.

It is this last development objective that motivates our proposal that funding for CCB efforts be linked with the OECD Development Assistance Committee (DAC) Programme of Official Development Assistance (ODA). There are clear political gains to be achieved here: the OECD-DAC allows the CCB component to be aligned with the ODA context, which is usually far less politically contentious than direct political subventions outside of ODA. Also, ODA sums can be immense – Norway, a world leader in ODA in terms of share of GNP, spent over USD 5.5 billion within the OECD-DAC context in 2013 alone, nearly half as much as the much larger German, and more than twice as much in terms of share of GNP.

As a world leader in ODA, Norway's engagement and initiatives in this area are watched closely. Norway was one of the first countries to actively pursue Security Sector Reform (SSR) projects, and its experiences have been used to inform many other countries in their work. Particularly instructive has been Norway's experience in work on Defence Security Sector Reform (DSSR), intelligence sector reform, and law-enforcement capacity building (See Caparini, Kjellstad and Nikolaisen, 2011.).

This section provides an overview of the OECD-DAC programme and the objectives it pursues. We then categorize the CCB activities that could be reported within an ODA framework. Compliance with these programmes allows funds that have been dedicated to CCB to count officially towards ODA commitments made. Essentially, this means that ODA-allocated funds may be used for CCB purposes without necessitating major budgetary changes. Funds that can officially be classified as overseas development assistance are colloquially referred to as being 'ODAble'.

3.1 The OECD DAC programme and ODA

The OECD-DAC provides in its Statistical Reporting Directives (known as CRS) the definition of the ODA system and the specifics of its reporting (OECD, 2013a). ODA is defined as 'those flows to countries and

territories on the DAC List of ODA Recipients and to multilateral development institutions which are:

i) provided by official agencies, including State and local governments, or by their executive agencies; and

ii) each transaction which:

a) is administered with the promotion of the economic development and welfare of developing countries as its main objective; and

b) is concessional in character and conveys a grant element of at least 25% (calculated at a rate of discount of 10%).

The OECD-DAC has existed since 1961, and has the mandate to 'promote development co-operation and other policies so as to contribute to sustainable development, including pro-poor economic growth, poverty reduction, improvement of living standards in developing countries, and a future in which no country will depend on aid.' It functions as an international forum with donor countries and recipient bodies.

These bodies may be either countries that are in the list of DAC members (OECD, 2013b) (when transactions are undertaken by a donor country directly with a developing country, the transaction is termed *bilateral*) or multilateral development institutions (OECD, 2013c) (in which case transactions are termed *multilateral* if they satisfy a set of criteria to ensure their multilateral character, or *multi-bi* or *earmarked* if they do not satisfy these criteria). In the case of a multilateral development institution, only the share of the contribution that corresponds to its development activities is reportable as ODA.

3.2 Which CCB activities qualify as ODA?

We now turn to the activities within our segmentation that appear most closely aligned with the goals of the specific list of activities that can be reported as ODA (*'ODAble'*). This is not meant as an exhaustive list, but as a list of activities that countries do today that they could start reporting as ODA. The CRS codes provided below are updated as of May 2015 (OECD, 2013c); see OECD (2013a) for explanation of the activities included.

Non security-related ODA activities

- **CRS CODE 22040 Information and Communication Technology (ICT)**: *Computer hardware and software; Internet access; IT training. When sector cannot be specified*. In fact, ODA includes all 'development-oriented social and cultural programmes (...) to enhance the social and cultural development of nationals of developing countries.' By enhancing the level of knowledge and

use of ICT and Internet-enabled technologies, those programmes foster a thriving business environment that will contribute heavily to the development of the economy. Methodological programmes designed for the civil society at large, notably to disseminate knowledge about the rule of law in cyberspace, might qualify as well for this kind of ODA.

⇢ Funding for technical support programmes designed to enhance Internet access and build cyber capacities, including the provision of hardware and software for civil society at large, such as all the funding for IXPs and trainings for the ISPs (see Box 5) is ODAble.

- **CRS CODE 99820 Promotion of development awareness:** *Spending in donor country for heightened awareness/interest in development cooperation (brochures, lectures, special research projects, etc.).* In fact, ODA includes research, defined as 'financing by the official sector, whether in the donor country or elsewhere, of research into the problems of developing countries. This may be either (i) undertaken by an agency or institution whose main purpose is to promote the economic growth or welfare of developing countries or (ii) commissioned or approved, and financed or part-financed, by an official body from a general purpose institution with the specific aim of promoting the economic growth or welfare of developing countries' (OECD, 2103a).

  → Funding for research projects in the field of capacity building, such as funding for Oxford's Global Cyber Security Centre from the UK FCO (see Box 6), is ODAble.

Security-related ODA activities

Various security expenditures included in the definition of ODA are particularly relevant for CCB activities. Therefore, the security/development nexus includes not only SSR activities but also all activities that can have an impact on SSR.

- **CRS CODE 15210 Security System Management and reform:** *Technical cooperation provided to parliament, government ministries, law enforcement agencies and the judiciary to assist review and reform of the security system to improve democratic governance and civilian control; technical co-operation provided to government to improve civilian oversight and democratic control of budgeting, management, accountability and auditing of security expenditure, including military budgets, as part of a public expenditure management programme; assistance to civil society to enhance its competence and capacity to scrutinize the security system so that it is managed in accordance with demo-*

cratic norms and principles of accountability, transparency and good governance.

→ **All activities at the intersection of CCB and SSR are ODAble and should be reported with this code.** This includes activities aimed at improving civilian oversight and democratic control of security expenditure (methodological support) and assistance to civil society to enhance its competence and capacity

- CRS CODE 15130 Legal and judicial development: *Support to institutions, systems and procedures of the justice sector, both formal and informal (…) maintenance of law and order and public safety; border management; law enforcement agencies, police, prisons and their supervision. (…) Measures that support the improvement of legal frameworks, constitutions, laws and regulations; legislative and constitutional drafting and review; legal reform; integration of formal and informal systems of law.* In fact, ODA includes 'expenditures on police training in routine civil policing functions, but not training in counter-subversion methods, suppression of political dissidence, or intelligence-gathering on political activities' (OECD, 2013a).

  → Technical support for LE-related teams, community-based instruments and methodological programmes around law enforcement issues is ODAble. This code should be used for activities that do not primarily target security system reform and are not undertaken in connection with post-conflict and peacebuilding activities.

The above list is by no means exhaustive. Other categories of the code 152xx (security-relevant codes) could be examined for their relevance for CCB. Of course, governments are always free to ignore these established programmes – there are many in the ODA community who would undoubtedly be unhappy about any efforts to re-position money away from established ODA activity to new ventures, let alone security-related ones. However, as the Netherlands has shown – as mentioned, funding for the GFCE initiative comes almost entirely from the ODA budget – there is much to be gained from working with existing structures. And the sums under consideration represent fractions of total ODA budgets.

3.3 Is 'ODAble' really 'doable'?

Is it in fact desirable to connect CCB with ODA? We have indicated several positive reasons why CCB is innately close to the established development agenda. In fact, most governments aspiring to implement CCB have (or will) connect them with the overall ODA framework. However, significant concerns should be kept in mind.

The idea of connecting the term 'cyber security' with the term 'development' (and especially with 'Internet governance') is contentious. From a development perspective, concerns on further 'securitizing' aid are sure to be raised. From an operational international security perspective, moving from established 'military–military' (or law enforcement, or similar) cooperative environments into the highly regulated and transparent ODA field entails certain challenges – among them, the prospect of not being able to compete with non-OECD countries that are not bound by the same stringent rules. Finally, many in Western Internet governance have been resisting any increased 'governmentalization', let alone 'securitization', of their field – and focusing CCB on Internet governance would confirm both these fears.

These concerns are not unfounded – in the worst case, government risks significantly impairing its ability to deliver highly needed assistance, while at the same time weakening both the ODA and Internet governance community. The first overriding benefit of a CCB programme linked to ODA can be easily summarized: the connection greatly facilitates access to funds. As yet, however, the sums for most CCB programmes are tiny – not even a fraction of most ODA budgets, making it doubtful that the tradeoffs are worth it at current budgetary levels. However, there is substantial scope for increasing average CCB budgets ten-fold, even twenty-fold, and that would indeed speak in favor of connecting it to the ODA field in general. If, however, such a budgetary commitment is not intended, or is even excluded in the longer run, then the entire 'development' focus of CCB will need to be revaluated.

There is a second and by no means minor benefit in connecting the OECD-DAC regime with CCB. And that, bizarre as it might seem from a traditional ODA point of view, is de-securitizing (or more importantly, 'de-militarizing') international cybersecurity, and putting a 'non-politicized, defence-oriented' view front and centre in the debate. Purely bilateral, non-aid related CCB efforts will doubtless be accompanied with accusations of favouritism and be perceived as part of the 'great power' struggle – for instance with donors insisting that only their IT products be used, or political equipment not be installed, or political positions be taken on the international stage. A cornerstone of the development community's approach has always been to – as far as possible – de-politicize the aid process, and make it needs-based above all. Arguably, this is what the international cyber security discourse urgently needs – acknowledgement that all actors would benefit from an overall increase in the basic level of cybersecurity and increased participation in Internet governance. Such a process seems able to underline the view of the Internet as a common resource (a 'common heritage of mankind' in international law), a view that claims that everyone should benefit from the Internet while emphasizing that everyone also needs to protect it.

4. Conclusions

Cyber Security Capacity Building (CCB) is a newcomer in the nexus of security and development. However, despite the undoubted complexity of the subject, it can be aligned within existing budgetary structures – in particular those currently used in connection with Security Sector Reform within the OECD-DAC context.

However, CCB is much more than a new addition to the traditional ODA family. There are three principle reasons why CCB is likely to grow in importance. First, it is becoming increasingly clear that a key factor for economic and social development (and therefore political stability) is access to cyberspace. This invariably means that cyber security becomes a central element in encouraging this access, and in ensuring that Internet growth is not jeopardised through criminal behaviour. Secondly, given the nature of the Internet, if countries in the rich industrialized world are to be able to respond to cyber-threats against their own nations, greater collaboration is needed with the developing world – which increasingly hosts the infrastructure and the actors behind malicious cyber-activity. Such collaboration is possible only if basic cyber security institutions and skills are available in the partner countries – and that is very much in the donor countries' direct interest. Thirdly, the increasingly politicized 'global struggle' for dominance over governance of the Internet is becoming a critical issue within international relations. With two opposing views as to how the Internet should be governed, the importance of the 'swing states' – nearly all within the developing world – rises. In view of this triple rationale (regional stability, national security, international diplomacy), CCB could easily become one of the most important activities in security and development in the future – especially given its relatively modest size today.[12]

The following recommendations, intended for Norway specifically, are also however applicable in general as well.

1. *Establish a CCB programme modelled on the UK approach*
   The UK approach is encapsulated in four dimensions that also form the basis of this study – methodological, technical, infrastructural, and budgetary. This segmentation is considered flexible and scalable for future purposes, and this study has taken these four dimensions as the 'common denominator' of all tasks needed to help a partner government develop the ability to respond to cyber-threats.

12 In 2015, the Dutch and UK governments, for instance, have calculated only some USD 2.5 million per year for CCB – sums that are, however, expected to rise sharply.

Each dimension has a slightly different constituency and delivery partner – the budgetary support dimension addresses governmental infrastructure and operational expenses, the infrastructure dimension addresses means to support private sector and telecommunications development, the technical dimension the individual skills and partnerships within cyber security, and the methodological dimension can deliver the rationale, methods, and evaluation of these programmes as well as providing guidance to partner nations on how to formulate overall national cyber security strategies. Here it should be recalled that the 'methodological' line item in the UK programme represents basic social science research, and is not restricted to the drafting of CCB methodologies per se.

2. *Utilize private-sector expertise to help deliver technical projects*
   A major challenge for many states (and especially Norway) in delivering DSSR-related projects has been the impossibility of outsourcing to non-governmental actors. Many governments were forced to support such projects by drawing on a (often relatively small) cadre of government civil servants.[13] In CCB, the converse would apply – most of the trained individuals would, by default, come from the private sector, and could easily be augmented by international private sector actors as well. While it is recommended that certain guidelines and recommendations (e.g., the kinds of certification methods to be taught) should be drafted by the appropriate government ministry or agency (in Norway, the NSM), implementation may be left almost completely to non-governmental actors.

3. *Support infrastructure development initiatives*
   Governments should examine their options in urging international financial institutions (IFIs) to expand on their existing projects supporting ITC infrastructure development. In particular, Norway should consider what other needs may exist that currently are not being met through IFIs – either due to the very small budgetary requirements or through lack of expertise. Larger initiatives should be given special consideration.

4. *Connect with non-CCB programmes dedicated to improving the business environment*
   The true benefits of the Internet for local businesses in the developing world are unlikely to be realized unless the core conditions for economic growth can be met. Investing in the rule of law, and in education, is also vital to the success of CCB programmes. Similarly, programmes to encourage small and medium-sized enterprises and other specific business finance projects, can closely align with the needs of CCB. All these related programmes should be consid-

13 For instance, DSSR projects put a relative manpower strain on the Norwegian Ministry of Defence (Caparini, Kjellstad and Nikolaisen, 2011)

ered and mapped before embarking on a comprehensive CCB programme.

5. *Support cyber security community resources*
   Most tools used globally by cyber security professionals have been developed by the security community itself. These tools are often provided free of service by CERTs, or maintained by non-governmental organizations centrally. By supporting these resources (which can be developed and provided anywhere) a CCB programme can make an important contribution – not only to the partner country, but to the global infosec (cybersecurity) community as a whole.

6. *Support both governments and civil society engagement in Internet Governance*
   Various resource constraints inhibit global participation in the multi-stakeholder approach. This applies equally to civil society as well as to governments – travel needs alone may represent an unsurmountable obstacle for participation in Internet governance. Donor countries have a range of options on how to engage here, such as providing budgetary support to government departments (in case of government support) or empowering local NGOs.

7. *Examine the possibility of 'sponsoring' a partner cyber security entity*
   The economics of the cyber security industry make it unlikely that developing countries can afford many good technical professionals – or retain them for long, if they train them internally. A compromise solution can be an outside organization that is run like a PPP – perhaps with the help of a local Internet registry or telecommunications company – and which can further be funded through a CCB programme. The costs of such an engagement can be sizeable and are currently outside of any known Western CCB programme, but the potential returns on investment are significant. It would be best to attempt such multi-year engagements only in regions where deep partnerships already exist, especially involving the security services or similar institutions.

8. *Leverage international ODA efforts to promote CCB*
   Norway has long been a trendsetter in international aid and development, and exercises great influence on how other nations allocate funds. Building on its experience with other ODA-specific innovations (such as SSR), Norway could contribute to raising the overall awareness of CCB projects within the wider ODA community. True, there are good reasons to be wary of connecting CCB with the ODA approach. If the size of the overall programme is not intended to exceed a very low threshold (a few percentage points of overall ODA flows), that significantly weakens the argument for linking CCB to ODA.

Cyber Security Capacity Building is a new field, and its budgets and concepts are as yet relatively undeveloped. However, this is bound to change – the cross-cutting importance of the Internet for economic and social growth, the relevance for donor-side national security, and the growing international relations and diplomacy perspective together provide powerful reasons for considering CCB. The question is not if donor countries will increasingly embark on such programmes, but when – and who will be the leaders defining this topic for the future. The question remains: which actors will be first in building these new partnerships – and which will be last?

Bibliography

Citizen Lab, Munk School of Global Affairs, University of Toronto (2013) 'Economic Cost of Cybercrime in Nigeria', at: https://www.pinigeria.org/download/cybercrimecost.pdf

Dalberg (2013) 'Impact of the Internet in Africa: Establishing Conditions for Success and Catalysing Inclusive Growth in Ghana, Kenya, Nigeria and Senegal', at: http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf

DCAF/ISSAT (2012) 'SSR in a Nutshell: Manual for Introductory Training on Security Sector Reform', at: http://issat.dcaf.ch/content/download/2970/25352/file/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf

ENISA (2006), 'A step-by-step approach on how to set up a CSIRT: Including examples and a checklist in form of a project plan', at: https://www.enisa.europa.eu/activities/cert/support/guide

ENISA (2008), 'Emergency Response to Security Breaches', at: https://www.enisa.europa.eu/activities/cert/background/files/CERTS_April_2008_hires.pdf

ENISA (2011) 'Proactive Detection of Network Security Incidents', at: https://www.enisa.europa.eu/activities/cert/support/proactive-detection

ENISA (2012) 'The Fight against Cybercrime: Cooperation between CERTs and Law Enforcement Agencies in the Fight against Cybercrime – A First Collection of Practices', at: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime

EUISS (2014) 'Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development' (edited by Patryk Pawlak), at: http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf

Goldsmith, Jack (2012) 'Cyber Security Treaties: A Skeptical View', at: http://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf

Hurwitz, Roger (2014) 'The Play of States: Norms and Security in Cyberspace' *American Foreign Policy Interets: The Journal of the National Committee on American Foreign Policy,* 36:5, 322-331

IC4D (2009) 'Extending Reach and Increasing Impact', at: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTIC4D/0,,contentMDK:22229759~menuPK:5870649~pagePK:64168445~piPK:64168309~theSitePK:5870636,00.html

IC4D (2012) 'Maximizing mobile', at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Report.pdf

ITIF (2012) 'The Benefits of ITA Expansion for Developing Countries', at: http://www2.itif.org/2012-benefits-ita-developing-countries.pdf

ITU [International Telecommunications Union] (2012) 'Impact of Broadband on the Economy', at: https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf

JOIN, European Commission (2013) 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

Klimburg, Alexander (2006) 'Watering the Grass Roots', at: http://en.collaboratory.de/w/Watering_the_Grass_Roots

Klimburg, Alexander (2014) 'Building a Pluralist Future for the Internet', at: http://www.atlanticcouncil.org/en/publications/articles/building-a-pluralist-future-for-the-internet

McAfee (2014) 'Net Losses: Estimating the Global Cost of Cybercrime', at: http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf

NIST (2014) 'Framework for Improving Critical Infrastructure Cybersecurity', at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Caparini, Marina, Kari Marie Kjellstad and Trine Nikolaisen (2011) 'A Stocktaking of Norwegian Engagement in Security Sector Reform' *NUPI report* at: http://brage.bibsys.no/xmlui/bitstream/id/320208/SIP11-Caparini+et+al-NUPI+Report.pdf

OECD International Futures Programme (2011) 'Reducing Systemic Cybersecurity Risk', at: https://www.oecd.org/gov/risk/46889922.pdf

OECD (2012) 'Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy', at: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

OECD (2013a) 'Converged Statistical Reporting Directives for the Creditor Reporting System (CRS) and the Annual DAC Questionnaire', at: https://www.oecd.org/dac/stats/documentupload/DCD-DAC%282013%2915-FINAL-ENG.pdf

OECD (2013b) 'DAC List of ODA Recipients', at: https://www.oecd.org/dac/stats/documentupload/DAC%20List%20of%20ODA%20Recipients%202014%20final.pdf

OECD (2013c) 'List of ODA-eligible International Organisations', at: https://www.oecd.org/dac/stats/documentupload/Annex%202%20for%202013.xls

OECD (2013d) 'DAC and CRS Code Lists', at: https://www.oecd.org/dac/stats/documentupload/DAC%20and%20CRS%20list%20of%20codes%20_may_2015.xls

United Kingdom Cabinet Office and National Security and Intelligence (2011) 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', at: https://www.gov.uk/government/publications/cyber-security-strategy

WEF [World Economic Forum] (2014) 'Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience', at: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

WEF [World Economic Forum](2015) 'Expanding Participation and Boosting Growth: The Infrastructure Needs of the Digital Economy', http://www3.weforum.org/docs/WEFUSA_DigitalInfrastructure_Report2015.pdf

White House (2015) 'FACTSHEET: U.S.–Japan Cooperation for a More Prosperous and Stable World', at: https://www.whitehouse.gov/the-press-office/2015/04/28/fact-sheet-us-japan-cooperation-more-prosperous-and-stable-world

This report is part of the project “Cybersecurity and Developing Countries”, funded by the Norwegian Ministry of Foreign Affairs.

The project has previously published “Cyber Security Capacity Building in Developing Countries: challenges and Opportunities, by Lilly Pijnenburg Muller. Available at www.nupi.no

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.

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

About the authors

Alexander Klimburg is a Nonresident Senior Fellow with the Cyber Statecraft Initiative of the Brent Scowcroft Center on International Security, a Senior Research Fellow at the Hague Centre for Security Studies, an Affiliate and former Fellow of the Belfer Center of Harvard Kennedy School, and an Associate Fellow at the Austrian Institute of European and Security Policy.

Klimburg has worked on numerous topics within the wider field of international cybersecurity since 2007. He has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and Internet governance. He has participated in international and intergovernmental discussions within the European Union and the Organization for Security and Co-operation in Europe and has been a member of various national, international, NATO, and EU policy and working groups, and has presented at NATO, the US Congress, and the European Parliament; and he regularly participates and organizes track 1/1.5 diplomatic initiatives as well as technical research groups. He is author and editor of over a dozen books, research papers, and commentaries, and has often featured in the international media, including in Newsweek, Reuters, and others.

Hugo Zylberberg (@hugozylb) is a Master in Public Policy candidate at Harvard’s Kennedy School of Government after graduating from Ecole polytechnique in France with a major in Economics. He is concentrating his studies on the political layer of the Internet, power in cyberspace, and cybersecurity. Hugo helped found The Future Society to help bring awareness of long-term technological problems and equip future policymakers to make better decisions and use technology instead of being used by technologists.