4. ORGANISATIONAL STRUCTURES & CONSIDERATIONS

Eric Luiijf, Jason Healey

Section 4: Principal Findings

- Essentially, national cyber security (NCS) can be split into five distinct subject areas or mandates. These 'Five Mandates' are Military Cyber, Counter Cyber Crime, Critical Infrastructure Protection (CIP) & Crisis Management, Intelligence/Counter-Intelligence, and Cyber Diplomacy & Internet Governance.
- These mandates can be mapped along all stages of a cyber incident, as well as all four levels of government: the political/policy, strategic, operational, and tactical/technical levels.
- Further, these Mandates connect with 'cross-mandates': Information Exchange & Data Protection, Coordination, as well as Research & Development and Education.
- While it is important to understand the uniqueness of each of the five mandates, it is even more important to understand their commonalities, and their need for close coordination.
- A wide range of organisations engage in international cyber security activities. The most relevant of these are often not state but non-state groups.
- A lack of understanding of the mandates can lead to stovepiped approaches resulting in conflicting legal requirements and friction between cyber security functions, organisations and capabilities.
- Assigning resources without a policy can be as dangerous as drafting a policy without assigning the resources.

4.1. INTRODUCTION

The purpose of this section is to review specific types of national cyber security (NCS) areas (also called 'mandates') and examine the organisational and collaborative models associated with them. Before discussing the wide variety of organisational structures at the national and international levels, a decomposition model will be presented that delineates both common and specific cyber security functions, capabilities, and responsibilities along three different axes (Section 4.2). On the one hand we will distinguish between five NCS mandates. This section expands Klimburg's[351] segmentation and supplements it by three additional cross-mandates. Other axes are the cyber security incident response cycle and the various levels of decision-making. This decomposition model shall assist the reader in understanding the rationale behind the functions, responsibilities, and capabilities of organisations involved in cyber security as entities which, over the years, have been shaped by the specific division of tasks between the government, its agencies, public organisations, associations, and private companies. Section 4.3 provides an overview of the stakeholders involved in the provision of cyber security.

Taking the decomposition model as the point of departure, Section 4.4 strives to determine the main focus of analysis along the five mandates mentioned in Section 1 and three cross-mandates. Building upon this framework, Sections 4.5, 4.6 and 4.7 introduce the common set of national and international organisations. It is important to note that these sections also pay due attention to the special tasks which may be recognised by, and assigned to, various organisational subunits or organisations all belonging to one and the same mandate, or to a single service organisation in one of the mandates with the aim of supporting the other mandates. Finally, Section 4.8 will discuss some organisational pitfalls and lessons identified when addressing cyber security at the national level.

4.2. DELINEATING ORGANISATIONAL FUNCTIONS, CAPABILITIES AND RESPONSIBILITIES

To position the many cyber security functions, capabilities and responsibilities at the national and international levels, an analytical framework can be useful for further discussion. While there are certainly a number of methods that can be employed, the approach applied here focuses on three closely connected building blocks: the NCS mandates and cross-mandates; a generalised tool to analyse organisational conduct at large, and the incident management cycle.

---

[351] See Klimburg in Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65)*. 15-9.

A first decomposition is to split the functions across the five perspectives (called mandates) as described at more length elsewhere[352] and in Section 1.[353] These mandates include: (1) Internet Governance and Cyber Diplomacy, (2) Cyber Crisis Management and Critical Infrastructure Protection (CIP), (3) Military Cyber Operations, (4) Intelligence/Counter-Intelligence, and (5) Counter Cyber Crime. This approach is supplemented by three additional cross-mandates that work across all the mandates equally. They include (1) Coordination, (2) Information Exchange and Data Protection, and (3) Research and Education.

4.2.1. Across the Levels of Government

An obvious, second way of decomposition is a vertical one, perpendicular to each of the mandates and cross-mandates. Along four distinct levels of analysis, this approach combines both a military and a political understanding of war.

The two probably most succinct (and opposing) notions on the nature of war equally address the most important relationship between the act of war and the political sphere: either '[w]ar is a mere continuation of policy',[354] or '[p]olitics is the continuation of war'.[355] It is long understood that it is necessary to combine the military and the political perspective into a more comprehensive approach of understanding conflict, such as was done in the US military construct of state-conflict.[356] By adding a 'political' or 'policy'[357] level on top of the traditional war-fighting triangle (which is composed of the strategic,[358] operational[359] and tactical[360] levels),[361] this model goes beyond a purely military understanding of military operations.

---

352 See ibid.

353 See Klimburg in Section 1.5.4.

354 Carl von Clausewitz, *On War* (London: Penguin Books, 1982 [1832]). 119.

355 Michel Foucault, *'Society must be defended': Lectures at the Collège de France, 1975-1976* (New York: Pan Books Limited, 2003). 15.

356 David W Barno, 'Challenges in Fighting a Global Insurgency,' *Parameters* 36, no. 2 (2006).

357 Defined as: 'principle or course of action' (see Policy, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

358 Defined as: 'the art of projecting and directing' (see Strategy, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

359 Defined as: 'a planned and coordinated activity involving a number of people' (See Operation, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

360 Defined as: 'skilful in devising means to ends' (See Tactical, *Oxford English Dictionary Online* (Oxford University Press, 2012)).

361 In the civil context, the operational and tactical levels of decision-taking are often reversed. In this section, however, we will use the military naming order: strategic, operational and tactical.

To go even further, it is suggested here that the four-level construct can be applied as an instrument to study the much broader context of organisational decision-making structures in government at large. As such, the four levels can be transformed into a more generalised analytical tool including: policy level where long-term political objectives are defined (e.g., a 'White Book' announcing cyber security as a top national priority); a strategic level where organisations are set up to achieve the predefined objectives (e.g., a directive establishing a specific body to achieve cyber security); an operational level where the different tasks within an individual organisation are coordinated (e.g., the segmentation of an organisation into different departments), and a tactical level where the specific tasks are ultimately executed (e.g., the specific tactics, techniques and procedures that are employed for each task). This delineation will be used for the positioning of organisational functions and capabilities only – in particular, to help provide possible examples for operational NCS institutions. Up front, it is important to remark that a strict separation of decision-taking processes into strategic-operational-tactical institutions does not necessarily reflect the actual reach of operational or tactical institutions. Effectively, a tactical level institution (say, a Computer Emergency Response Team within a crisis management unit) can take decisions that have global consequences, impacting not only the strategic but also, potentially, the political level as well.

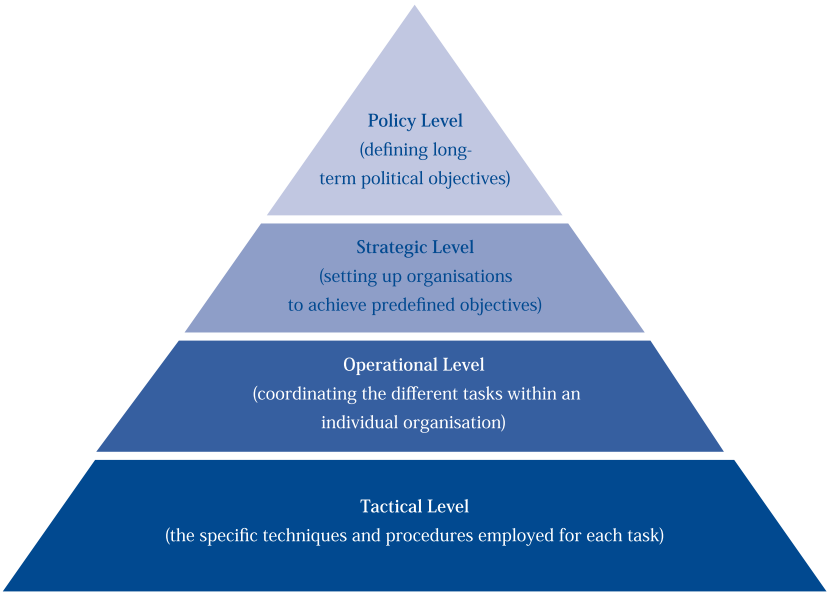

Figure 3: The Four Levels of War as a Generalised Tool for Analysis

It is required that the organisational responsibilities are assigned at each of these levels. In many cases, however, a clear distinction between the various levels can be difficult. Sometimes specific tasks (at the tactical level) are 'bolted on' to the organisations or to strategic goals to which they are only partially suited. Indeed, this misalignment of specific tasks to unsuited organisations, levels or even mandates is a major challenge for national cyber security. The organisational embedding of a national Computer Emergency Response Team (CERT) function[362] in a number of nations is a good example of such a misalignment. In various nations, the government CERT function has been a quick fix add-on to an existing government organisational structure. Often, this crucial tactical function is not tied into the most appropriate vertical decision-making structure or, indeed, within the best horizontal connections. For instance, one European national CERT is attached to the Ministry of Finance – a ministry that has effectively nothing in common with the particular mission of a CERT as described by CERT/CC at Carnegie Mellon University.[363, 364] However, there are numerous examples where a government CERT will, for instance, not receive specific intelligence as it is not part of the right governmental information channel, even though they are often the only body that can actually act on this intelligence. This in turn limits the effectiveness of national-level CERTs, leading other departments to duplicate their activities which can ultimately lead to a 'function creep' with an inter-agency conflict as a result.

4.2.2. Across the Incident Management Cycle

A third method of delineation is to distinguish the cyber security functions, capabilities and responsibilities along the so-called 'incident management cycle'. The 'plan-resist-detect-respond'[365] security incident management cycle is one popular approach that has been specifically been adapted to information security.[366] This

362 Described within the present context as 'tactical' function, although, in fact, a CERT/CSIRT is essentially an 'organisational' unit with its own specific subordinate tasks (see Section 3.1.4). In essence, a CERT is group of people in an organisation who coordinate their response to breaches of information security or other computer emergencies such as breakdowns and disasters. Other accounts also refer here to a Computer Security Incident Response Team (CSIRT), a Computer Incident Response Team (CIRT) or just Incident Response Team (IRT). A CERT is a highly scalable entity: it can range in size from a single part-time employee without an assigned workstation to an organisation with hundreds of staff providing 24/7 services from a hardened facility.

363 See Carnegie Mellon University, 'About Us'.

364 Robert Bruce et al., International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680), (Delft: Tuck School of Business at Dartmouth, 2005), http://www.ists.dartmouth.edu/library/158.pdf. vii, and 77-80.

365 Lenny Zeltser, 'The Big Picture of the Security Incident Cycle,' *Computer Forensics and Incident Response*, 27 September 2010.

366 See, for instance, NITRD, 'Interagency Working Group on Cyber Security and Information Assurance (CSIA IWG),' NITRD, https://connect.nitrd.gov/nitrdgroups/index.php?title=Interagency_Working_Group_on_Cyber_Security_and_Information_Assurance_%28CSIA_IWG%29.

cycle closely resembles the traditional emergency management cycle (comprising four elements: mitigation, preparedness, response and recovery), a cycle which is often found in the US emergency management literature and functional planning.[367]

In Europe, four or five elements are recognised in making up the cyber security incident management cycle: pro-action, prevention, preparation, response and recovery. Response and recovery are sometimes combined into a single element: suppression. Some nations, like the Netherlands, recognise another essential sixth element: aftercare/follow up.

The lack of a uniform structure for incident, emergency and crisis management is reflected by a wide variety of definitions for each of these elements in the security management cycle.[368, 369] For the decomposition approach this will not be a problem as, in this section, it is only needed to understand the functional placement of NCS functions, capabilities, and responsibilities along the incident response cycle.

Pro-action: defined as 'activities that reduce or remove the structural causes of insecurity.'[370] Pro-action comprises carrying out a national risk assessment (NRA) for the cyberspace domain, establishing a legal framework for cyber security, and an organisational framework. The NRA may identify insufficient and non-existing, but required, cyber security capabilities. It is up to the policy level to decide when this identified gap is filled (or not).

Prevention: in an emergency management context this has been defined as 'actions to avoid an incident or to intervene to stop an incident from occurring.'[371] For the purposes here, we use a slightly different definition: 'actions to prevent hazards from developing into incidents altogether or to reduce the effects of possible incidents'. Preventive cyber security measures reduce vulnerability to the global cyberspace and to individual NCS in particular.

Preparation: defined as 'planning, training and exercising' or as 'a continuous cycle of planning, organising, training, equipping, exercising, evaluating, and taking

---

367 See, for instance, Michael K. Lindell, Carla S. Prater, and Ronald W. Perry, Fundamentals of Emergency Management (Washington, DC: FEMA, 2006), http://training.fema.gov/EMIWeb/edu/fem.asp.

368 ICDRM, Emergency Management Glossary of Terms, (Washington, DC: George Washington University, 2010), http://www.gwu.edu/~icdrm/publications/PDF/GLOSSARY%20-%20Emergency%20Management%20ICDRM%2030%20JUNE%2010.pdf.

369 Dutch Ministry of Housing, Spatial Planning, and the Environment, Handreiking Security Management, (The Hague: Dutch Ministry of Housing, Spatial Planning and the Environment, 2008), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/11/26/handreiking-security-management/11br2008g225-2008613-154851.pdf. 23.

370 Ibid.

371 ICDRM, *Emergency Management Glossary of Terms*. 76.

corrective action in an effort to ensure effective coordination during incident response.'[372]

Response: addresses the immediate and short-term effects, and prevents further damage after an incident occurs.[373]

Recovery: this encompasses 'activities and programs implemented during and after response that are designed to return the entity to its usual state or to a 'new normal'.'[374]

Aftercare/follow up: takes into account the psycho-sociological impact of an incident to (parts of) the population, covers incident and incident management investigation (such as fact finding and the writing of lessons identified), as well as forensic analysis, criminal investigation and the prosecution of suspects.

The security incident management cycle stems from an understanding that the lessons identified during the preparation (through aftercare/follow up) need to be converted into lessons learned.[375] These can subsequently either be adapted as a strategy and policy (pro-action), lay the foundation for new or revised prevention measures and approaches, help to develop and implement new or changed preparation measures (e.g., exercise programme), or can usefully be employed to implement and train changed procedures and processes that are part of the incident response element of the cycle.

Below, we will use this six elements model to discuss common and specific functions, capabilities and responsibilities at the national level.[376] The functions and capabilities placed in the six elements model can easily be mapped by the reader to one's national cyclic five or four elements model if required.

4.3. CYBER SECURITY STAKEHOLDERS

A wide range of stakeholders either provide or interact with cyber security functions, both at the national and international levels. These stakeholders are the same ones identified in the previous section: governmental, national/societal and

---

372 US Department of Homeland Security, National Incident Management System, (Washington, DC: FEMA, 2008), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf. 145.

373 ICDRM, *Emergency Management Glossary of Terms*. 85-6.

374 Ibid., 82.

375 Note the distinction between 'lessons identified' and 'lessons learned'.

376 This 'operational' perspective includes the (inter)national functions, capabilities and responsibilities, and not at the tactical level of cyber security organisations which is internal to a department, agency, or other organisation.

international/transnational. Similar to what is described in the previous section, stakeholders are not necessarily constrained within each category but can operate with multiple 'hats'. For example, a government body may act as an end-user (Whole of Nation); help develope a digital certificate for service providers (Whole of System), and establish regulation (Whole of Government). Therefore, we use the following three non-exhaustive sets:

- Governmental:
  - the national government, its public and semi-public agencies,
  - independent regulatory bodies,
  - inspectorates dealing with cyber security aspects for their top-level domains,
  - the military, and
  - local government/administration & municipalities;
- National/Societal:
  - critical infrastructure (CI) sector organisations & operators,
  - ICT service providers (e.g., Internet Service Providers (ISP) & cloud services),
  - industry and businesses at large (and their branch organisations),
  - small and medium enterprises (SME),
  - (national) software and hardware manufacturers and system integrators,
  - universities and research & development organisations,
  - specialised defence and security contractors,
  - the population at large;
- International/Transnational:
  - multinational arrangements & bodies (e.g., G8, EU, OSCE,[377] ITU, World Bank, Europol, Interpol),
  - multi-stakeholder institutions (e.g., IGF,[378] ICANN[379]),

377 OSCE = Organisation for Security and Co-operation in Europe.

378 IGF = Internet Governance Forum.

379 ICANN = Internet Corporation for Assigned Names and Numbers.

- international standardisation bodies (e.g., FIRST, ISO[380]),
- informal international arrangements (e.g., IETF,[381] IEEE),
- key global infrastructure providers (e.g., backbone providers), and
- key global software and hardware manufacturers.

When discussing specific cyber security functions, capabilities and responsibilities in the following sub-sections, this list of stakeholders will be referred to when applicable.

4.4. MAIN FOCUS OF ANALYSIS

4.4.1. Along the Mandates

Figure 4 shows the generic model with the six elements of the cyber security cycle versus the five mandates as defined by Klimburg[382] and introduced in Section 1. The elements of the cyber security incident management cycle for each mandate which are not key at the national level are suppressed in the figure.

The internet governance/cyber diplomacy mandate acts across all of the incident cycle elements, such as international pro-active arrangements; harmonised prevention actions; exercises to be prepared for a hot phase response, and seeking international support during a hot response-recovery – follow up phase. The activities are mainly positioned at the policy/strategic levels.

The two areas of the cyber security crisis management and CIP mandate require a split. Cyber security crisis management requires a set of operational and tactical level functions for the preparation, response, recovery and aftercare/follow up elements of the incident response cycle, whereas the CIP strategic through tactical focus lies with prevention. The preparation through recovery elements are covered to mitigate the exposure in case prevention fails.

The military cyber operations mandate, above all, needs to protect its own cyber infrastructure. However, this is an internal organisational issue. At the national level, military cyber operational response and recovery capabilities need to be prepared (tactically and operationally) for countering cyber attacks against one's

380 ISO = International Organization for Standardization (www.iso.ch).

381 IETF = Internet Engineering Task Force – leads the internet protocol standardisation efforts.

382 See Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).*

nation. These capabilities may include both pre-emptive cyber strikes and (counter) attacks.

As part of their tasking, military cyber defence capabilities may be involved in the cyber protection of international alliances such as NATO and the EU. Currently, frameworks for collective military cyber defence operations do not exist or have not been made public. However, the Dutch government endorsed the view that:

> 'Under international law, the use of force in self-defence pursuant to Article 51 of the UN Charter is an exceptional measure that is justified in armed cyber attacks only when the threshold of cyber crime or espionage is breached. For a cyber attack to justify the right of self-defence, its consequences must be comparable with those of a conventional armed attack. If a cyber attack leads to a considerable number of fatalities or large-scale destruction of or damage to vital infrastructure, military platforms and installations or civil property, it must be equated with an 'armed attack'[383]

and:

> 'An organised cyber attack on essential state functions must be regarded as an 'armed attack' within the meaning of Article 51 of the UN Charter if it causes (or has the potential to cause) serious disruption to the functioning of the state or serious or prolonged consequences for the stability of the state, even if there is no physical damage or injury. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks.'[384]

It concludes that 'Articles 4 and 5 of the North Atlantic Treaty may be applied to attacks in cyberspace. Article 5 is worded so generally that it can cover all forms of armed force. Article 4 is not as extensive in scope and may be applied to cyber attacks that endanger national security but do not breach the threshold of an armed attack.'[385] Therefore, collaborative cyber defence against a hostile actor causing a major cyber disruption to one or more nations of the Alliance is considered to be covered under the current North Atlantic Treaty.[386]

---

383 AIV/CAVV, Cyber Warfare, (The Hague: AIV, 2011), http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf.

384 Ibid.

385 Ibid.

386 For a further discussion on this, see Section 5.3.

The (counter-) intelligence mandate, first and foremost, focuses on prevention: the timely understanding plans and techniques of potential lone wolves, activists, terrorists, and adversary states. In case prevention fails, intelligence has to attribute attacks to specific attackers as part of response and follow up. Cyber security has been added as a new domain to the existing set of (counter-) intelligence activities which are mainly placed at the tactical/operational level. When applied, cyber security counter-intelligence is a preventing task by nature. However, the counter-intelligence capability may include offensive disruption tasks, when applicable.

The counter cyber crime mandate requires specific strategic and operational pro-action activities, and operational and tactical activities for all other elements.

Figure 4: The Five Mandates and the Six Elements of the Cyber Security Incident Cycle Model

4.4.2. Along the Cross-Mandates

In addition to the NCS mandates we also identified three cross-mandates. As is shown in Figure 5, the cyber security coordination cross-mandate crosses all of the five NCS mandates. At the political level this is synonymous with the overall coordination and control of NCS efforts. At the strategic and operational level it is primarily concerned with avoiding duplication of efforts, while at the tactical level it refers to the need to connect various tasks with each other.

The cyber security information exchange and data protection cross-mandate function has its main information exchange focus in prevention, response and recovery, and is active across all levels of activity. While at the tactical level it is important to exchange technical information on cyber threats, vulnerabilities and attacks, the sharing of intelligence at the very top of government and with private industry (e.g., critical infrastructure operators) when required, is no less important. However, most of the time, operational information exchange will occur during preparation and aftercare/follow up by specific organisations such as national crisis management and investigation organisations, respectively. Proper data protection processes are a pre-condition for operating cyber systems. The main focus is driven by the political/policy side, which must ensure the appropriate application of guidelines (OECD)[387] or legislation (e.g., within the EU[388]) across all forms of information exchange. This is supervised by Data Protection ('Privacy') Authorities[389] which keep the oversight as regulators at the operational level or working within the legal advisory frameworks of the relevant institutions (such as within the intelligence services). It is important to note that information that has been gathered in clear breaches of applicable data protection legislation can be sufficiently 'contaminated' that foreign partners may not want to use it – effectively depriving that respective nation of valuable diplomatic currency.

Cyber security research and development (R&D) and education (which includes awareness) form the third cross-mandate. Although each mandate may have its own R&D and education requirements and activities, cyber security awareness and education at the (inter)national level can effectively be organised across the five cyber security mandates to avoid duplication and waste of efforts. This cross-mandate capability will often be connected within an overall national and international R&D context (e.g., in researching internet security issues). Thus, it is primarily an (inter)national prevention capability. However, on the one hand

---

387 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

388 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal, L 281.A new draft Directive is being worked on in 2012.

389 For example the Information and Privacy Commissioner in Ontario, Canada: www.ipc.on.ca.

it is also a very important 'pro-action' capability supporting efforts for national risk assessment. On the other hand, it includes the development of, for instance, awareness campaigns about cyber security for specific population groups.

Figure 5: The Cross-Mandates and the Six Elements of the Cyber Security Incident Cycle Model

4.5. THE FIVE MANDATES OF NATIONAL CYBER SECURITY

Based on the previous work of Klimburg[390] and using the combined model outlined above, it is possible to position the common and specific cyber security functions along specific mandates/cross-mandates and the cyber security incident management cycle (figures 4 and 5). Also, it is possible to distinguish common cyber security functions and capabilities at the national level from specific functions which may be needed and fit only specific nations.

Before discussing the figures in more detail, it should be remarked that this is the optimal, clean sheet positioning of the cyber security functions – a theoretical best practice. As discussed by Klaver et al.,[391] a nation shall keep in mind that its existing national (and international) organisational frameworks and the functional division between departments, agencies and public bodies gradually developed over a long period of time based on historic, cultural, legal, political and other reasons. In every nation there will be a number of specific local conditions that determine the current placement of functions and the course of existing institutions. Consequently,

390 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).*

391 See, for instance, Klaver, Luijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe.* 10-1.

a transposition of the theoretical best practice institution to a country's local conditions situation is certainly required.

4.5.1. Military Cyber Operations

The cyber security functions resident within the military domain differ from nation to nation, as the exact definition of military cyber operations will also differ. Overall, this mandate can include a very wide range of sub-mandates, not all of which will be applicable in every nation. Firstly, this includes 'cyber defence' – the protection of its own ICT systems, usually with a CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) type of organisation in the lead and heavily dependent upon intelligence networks. Secondly, it can include options for strategic cyber operations – the ability to wage a 'cyber war' on the war fighting capability of the enemy.[392] Thirdly, it can include specific 'battlefield cyber capabilities' – those that are deployable within an operational and tactical battlefield environment (for instance against an enemy air defence system). Fourthly, it can include the modernisation efforts of more traditional military capabilities, such as those associated with Network Centric Warfare (NCW). It is important to note that the mandate may not only be national: a military cyber organisation may receive a mandate to support that nation's allies (e.g., within NATO) in an extension to its common security task. Apart from cyber defence (preparation, response and recovery), this may also include pre-emptive strike capabilities against a clear and present threat, counter-attack (response), or even an offensive capability mandate.

In case of a domestic national emergency, some nations have legal provisions for empowering the military to assist in emergency management, and help provide for internal security. Some of the military cyber security capabilities may, therefore, be trained to protect the 'homeland's cyberspace' in case the normal crisis response exhausts its resources to counter a cyber security crisis. The operational/tactical[393] command and control chain of the provided military cyber capability is, however, usually subordinate to the civil response authorities.[394]

Some nations (e.g., the United Kingdom and the Netherlands) organise their operational/tactical military cyber security response force in a flexible way. Others

---

392 See, for instance, Gregory Rattray and Jason Healey, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use,' in *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, ed. National Research Council (Washington, DC: The National Academies Press, 2010).

393 Note that the operational and tactical levels are reversed in the military structure as compared to civil structures.

394 France, the Netherlands and Switzerland are but three countries as an example.

(such as Estonia[395]) have created reservist or paramilitary cyber organisations that can provide reinforcement for regular military cyber forces in an emergency. These approaches are particularly useful given the inability of most nations to actually maintain all potentially required technical cyber skills in their organisation at all times.

4.5.2. Counter Cyber Crime

The counter cyber crime mandate comprises a wide set of organisations. At the policy and strategic levels, a ministry of justice is involved in the national, and often international, development and maintenance of cyber security legislation. Similarly, a ministry of the interior will often manage the dedicated police resources. Unlike in other mandates, however, some of these capabilities may well reside at a 'local' (provincial) governmental level, and not only be the responsibility of the central government.

Cyber crime prevention is a multi-angled issue. From the economic perspective, a ministry of economic affairs may manage cyber security awareness at the operational level and development programmes against cyber crime. Note that this overlaps with the R&D and education cross-mandate to be discussed later.

From the Whole of Government (WoG) perspective, state security and cyber crime prevention is an organisational issue across all government department and agencies. Currently, nations increasingly assign this strategic/operational responsibility to a Chief Information (Security) Officer (CIO or CISO) who has to develop, maintain and monitor government-wide information and cyber security policies.

From the perspective of secure service provisioning to the public at large, non-governmental service organisations such as ISPs may actively disrupt the spread of malware and other cyber crime activities. Public-private organisational arrangements such as an ISP Code of Practice and the identification of compromised customer systems exist in Australia,[396] and there are a number of anti cyber crime organisations that represent a mix of state and non-state actors.[397]

---

395 The Estonian 'Cyber Defence League' has, for instance, about 150 experts on call if necessary (see: Estonian Ministry of Foreign Affairs, 'Around 150 Experts Associated with Estonia's Cyber Defence League,' *Estonian Review*, 3 October 2011.).

396 Australian Attorney-General's Department, *Cyber Security Strategy*: 18-20.

397 One of these is, for instance, the Anti-Phishing Working Group (APWG). On a higher level, many of the top international network operators and similar technical experts regularly cooperate in a number of closed information exchange groups.

At the operational/tactical level, a police function is needed to investigate cyber crime, to try to take cyber criminals into custody, and have them prosecuted. This function extends across the preparation (training and exercises), response, and recovery elements. Logically, this function is embedded as a special knowledge area in the national police and local police forces. Cross-links and information exchanges with foreign police forces exist, either based on bilateral collaboration, or via the high-tech crime/cyber crime units of international police organisations such as Europol and Interpol.

To be effective, the police organisation may tie in with the national (and other) CERTs and public-private Information Sharing and Analysis Centres (ISACs) discussed under the cyber security crisis management & CIP mandate (Section 4.5.2). A common challenge is that, for many police forces, the act of starting a criminal investigation can put a sudden stop to information exchange that might help others. The public-private information exchanges and CERT organisations (Section 4.5.2) mostly deal with counter cyber crime prevention and response activities, and less often with the business continuity (or continuity of government) aspects managed under cyber security crisis management.

As part of the follow up, the national prosecution organisation has to extend and maintain its knowledge about cyber crime to operationally take care of the prosecution of cyber criminals as part of its normal way of operation. The forensic collection and analysis of data capability may (partially) be assigned to the police organisation. Some nations, however, have a national forensic service which covers, amongst other domains, the cyber security domain as well.

4.5.3. Intelligence/Counter-Intelligence

Distinguishing cyber espionage from cyber crime and military cyber activities is not uncontroversial. In fact, they all depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (both regarding intellectual property as well as government secrets) are in a class of their own. At the same time, it can be very difficult to ascertain for sure if the perpetrator is a state or a criminal group operating on behalf of a state, or indeed operating on its own.

Irrespective of who is actually behind the attack, cyber espionage probably represents the most damaging part of cyber crime (if included in the category). Lost intellectual property, for instance, was said to have cost the British economy £9.2 billion in 2011.[398] Cyber espionage, when directed toward states, also makes

[398] Michael Holden, 'Cyber crime costs UK $43.5 billion a year: study,' *Reuters*, 17 February 2011.

it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor nature in cyberspace. At the same time, counter-intelligence activities (e.g., detecting and combating the most sophisticated cyber intrusions) very often will depend upon other types of intelligence activity, including offensive intelligence collection but also extensive information sharing between international partners.

Collecting information through cyber means is just an extension of the existing set of capabilities being used by these services. Mostly, intelligence collected by other means will be used to address cyber security threats. The main focus is the defence of government systems from advanced cyber threats by state and non-state actors. Common tasks include information collection, verification, aggregation, analysis and dissemination.

Some nations allow their intelligence services to exploit the information for other purposes, or directly intervene in order to prevent threats from (re)occurring.[399] It is also possible that a specific vulnerability (and, therefore, an attack vector on a different organisation, such as a private company) will intentionally not be disclosed in order to further specific intelligence needs. Overall, intelligence and counter-intelligence organisations will concentrate their work within the operational/tactical environment but they will play an important role on the strategic level as well, especially in conducting regular threat assessments and the like. They are thus concentrated in the preparation and response phases.

4.5.4. Cyber Security Crisis Management and CIP

Cyber security crisis management comprises at least an operational and a mostly tactical function which spans the preparation (e.g., training & exercises), response, recovery, and aftercare/follow up elements of the cyber security incident management cycle. At the tactical level, a national computer emergency/security incident response team (CERT/CSIRT)[400] is required which preferably is fully linked to the national emergency/incident management structure at the political/strategic

---

399 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space.*

400 Bruce et al., *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680).* 112-3 and Appendix B.

level.[401, 402] Serious cyber incidents may lead to major disturbances and disruption of society. Incidents in, for instance, critical infrastructure sectors (such as energy and telecommunication) may have a serious impact at a national level when critical functions of cyberspace fail.[403] Moreover, the national emergency/incident management capability is closely connected to the national crisis communication capabilities, a function which comes in handy to communicate to the society and population about a serious cyber security incident at the (inter)national level.

At the operational level, there is often only a limited amount of integration due to legal reasons. For instance, in many nations there is a separation between the government CERT and the national CERT. The national CERT will often not be under direct control of the government, and will largely only have advisory functions. The government CERT does have (to various extents) operational control over the networks and network connections within its constituency, and is increasingly being used as the tactical level national cyber crisis management facility. Examples of such an arrangement can be found in Germany, the UK, the Netherlands, and many other countries.[404]

Different from cyber security crisis management, critical infrastructure protection (CIP) activities put their main focus on prevention. These are substantial governmental tasks, and a number of countries have set up dedicated CIP organisations, often with close connections to the internal security services.[405] This requires tools such as a national risk analysis[406] with perhaps corresponding national risk registries and regularly conducted assessments of specific risk factors

---

401 This means that the top crisis management advisory group (e.g., COBR in the UK) have NCS fully integrated into it.

402 It shall be noted that cyber-related emergencies with a serious national impact, but with different escalation characteristics, may occur more often than other emergencies. National cyber incidents may require a more flexible escalation process which may not require additional legal 'emergency' powers to deal with every single cyber-incident of national significance. To avoid a 'permenent state of emergency' it is necessary to re-conceptualise the tasks of 'national crisis management' to also include 'national incident management'. An equivalent level of emergency in another domain may be dealt with by a regional crisis centre, but the nature of cyber incidents at the national level may require the response of the national crisis response function.

403 For a concrete analysis of the economic effects of a major power outage, see: Public Safety and Emergency Preparedness Canada, Ontario – U.S. Power Outage – Impacts on Critical Infrastructure, (Ottawa: Public Safety Canada, 2006), http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-e.pdf. More recently, an Austrian study was one of the few attempts to examine the consequences of a national blackout, see: Johannes Reichl and Michael Schmidthaler, Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle, (Linz: Johannes Kepler Universität Linz, 2011), http://energyefficiency.at/web/projekte/blacko.html.

404 For a list of European CERTs and their constituents/stakeholders, see: ENISA, 'CERT Inventory,' ENISA, http://www.enisa.europa.eu/activities/cert/background/inv.

405 Examples of such organisations include the CPNI in the UK, and the CNPIC in Spain.

406 For a UK example, see: UK Cabinet Office, 'Risk Assessment,' UK Cabinet Office, http://www.cabinetoffice.gov.uk/content/risk-assessment.

to specific objects, organisations or processes/services. Secondly, it requires the development or adoption of information security standards or legislation within both the government and the private sector. Implementing information security practices[407] – perhaps the single the most basic and essential task within NCS – can be difficult to accomplish across central government, let alone the associated private sector critical infrastructure. Some countries simply proscribe the use of specific information security practices,[408] while some countries have more comprehensive legislation.[409] A third preventive tool, particularly for cyber security, is the information exchanges between the various actors. One approach[410] differentiates between three types of information exchanges. Firstly, a 'third party' model, which only involves exchanges between the non-state actors and without any government presence. Secondly, a 'community' model[411] that is usually sponsored by the government and security services, and provided with limited amounts of intelligence on threats, but not controlled by them. An example of this arrangement is provided by the UK Warning, Advice and Reporting Points (WARPs), or the Dutch Information Sharing and Analysis Centres (ISACs).[412] Finally, the 'hierarchical' model of information exchange is maintained by the government. It routinely delivers classified information to selected private organisations and companies. Examples of this arrangement can be found within France, Spain, the UK, the USA and a number of other countries. Particularly when these information exchanges are set up as public-private partnerships, they can further be connected internationally.[413] The national crisis management capability may be closely linked with the information exchanges. For all of these relationships, however, a considerable amount of trust between the various state and non-state actors is a necessary condition, and trust can only be built over time.[414]

---

407 For examples of approaches to information security, see Section 1.3.

408 For instance the German *Grundschutz* approach, or the French EBIOS tool.

409 One of the most extensive legislative examples is the 2002 US Federal Information Security Management Act (FISMA). FISMA is supported by a wide range of tools and services and aims to provide for standardised levels of information security across the civilian US federal government systems.

410 Sam Merrell, John Haller, and Philip Huff, Public-Private Partnerships: Essential for National Cyber Security [Transcript], (Pittsburgh, PA: Carnegie Mellon University, 2010), http://www.cert.org/podcast/show/20101130merrell.html. 5-7.

411 See, for instance, Austrian Federal Chancellery, *National ICT Security Strategy Austria*: 16.

412 See: WARP, 'WARP – Protecting our information infrastructures,' CPNI, http://www.warp.gov.uk. See also CPNI.NL, 'Werkwijze ISACs,' CPNI.NL, https://www.cpni.nl/informatieknooppunt/werkwijze-isacs.

413 An example of this is the European Public Private Partnership for Resilience (EP3R) maintained by the EU.

414 Klaver, Luiijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe*. 10-11.

4.5.5. Internet Governance and Cyber Diplomacy

Internet governance[415] builds on an infrastructure of non-governmental driven self-regulation, in which the internet grew bottom-up with a minimum of government and public sector influence. Internet volunteers and experts organised themselves to drive the architectural and protocol development of the internet in self-organising structures such as the Internet Architecture Board (IAB) or the Internet Engineering Task Force (IETF). The internet-only part of cyber security is just one of the topics dealt with in internet governance but, despite different initiatives, no single organisational body drives the rate of progress on security issues.[416] The main activity areas are related to pro-action/prevention, including the standardisation of security options in protocols, the development of specially designed cyber security protocols, and describing and standardising good tactical/operational practices. ICANN is one of the most important organisations within internet governance, and is responsible for coordinating activities to secure the core functionality of the internet and the global routing and naming infrastructure. Increasingly, incident response to cyber attacks on the basic backbone infrastructure (in particular the routing protocols) may require a globally operating operational and a distributed tactical incident response, recovery and follow up capability. ICANN has made proposals for a type of global crisis management capability[417] and the ITU has made some suggestions along these lines as well.[418]

Cyber diplomacy[419, 420] is considered here to be the general formal state engagement of a nation's diplomatic processes in the overall theme of global cyber security. In particular, this refers to multilateral or bilateral activity aimed at managing state-to-state relationships in cyberspace. Within the context of the United Nations, for instance, the Group of Government Experts (GGE) have been working on issues of international law of armed conflict in cyberspace, and are currently drafting principles for norms and standards of acceptable state behaviour. In 2012, the OSCE started a process to specifically create 'Cyber Confidence Building Measures'. A large number of other initiatives exist, both hosted by international or

---

415 A definition of internet governance can be found in: WSIS, *Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E)* (Tunis: ITU, 2005). Para 34.

416 It is true that there have been several attempts to deal with cyber security issues within internet governance. However, despite the security activities performed by DNS-OARC, ICANN's Security and Stability Advisory Committee (SSAC), its DNS Security and Stability Analysis Working Group (DNSSA-WG), or the valuable inputs delivered by the annual Internet Governance Forum (IGF) and many others, it is not entirely clear where the organisational responsibilities overlap and where better coordination is needed.

417 In particular, the need to establish a global 'DNS-CERT' or similar.

418 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).* 25-6.

419 Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, 7.

420 Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).* 18-9.

multilateral organisations (for instance, G8, OECD, etc.) or even stand-alone (such as the Meridian Group).[421] At the bilateral level, a number of 'major cyber nations' have conducted so-called Track 1.5 discussions on ways for reducing tensions in cyberspace. Cyber diplomacy is thus more equivalent to traditional diplomacy activities such as arms control and counter proliferation. Cyber diplomacy should not be equated with 'e-diplomacy', which is more concerned with the delivery of government messages using 'new media' – even though there might be important overlaps. For instance, in 2012, China[422] accused the US Embassy in Beijing of violating the Vienna Convention on Diplomatic Relations,[423] as the Embassy was 'automatically' broadcasting air quality for Beijing via Twitter.[424]

When it comes to designing structures for cyber diplomacy and internet governance, most nations find it difficult to assign specific responsibilities where they belong or take them away from where they have 'historically' been situated. For instance, internet governance – which is largely still totally separate from cyber diplomacy – is often dealt with by a ministry of economics or infrastructure, and is rarely involved in NCS issues. For many civil servants it can be difficult to perceive the larger picture within international cyber security, in particular, the view beyond their own department or mandate. This can often go hand-in-hand with a substantial lack of technical understanding. The challenge is particularly acute when dealing with 'bottom-up' internet governance organisations such as the IGF, IAB, IETF, IEEE and others – organisations that are still largely staffed by volunteers who often seem to speak a completely different language than government officials.

Moreover, government officials often lack insight into which of their national experts are playing key roles in the international organisations.[425] Although internet governance is perhaps the leading example of a topic requiring a Whole of System (WoS) coordination, it has proven to be very difficult for governments to adequately find their way in the existing 'multi-stakeholder' environment. As a consequence, there has been increasing governmental support for an 'intergovernmental' solution to internet governance (e.g., one in which the non-state sector would play only a supporting role). This is despite the stated claim of most liberal democracies to keep the internet 'free from government control'.

---

421 For a list of relevant organisations, see: US Government Accountability Office, Cyberspace. United States Faces Challenges in Addressing Global Cybersecurity and Governance, (Washington, DC: US Government Accountability Office, 2010), http://gao.gov/assets/310/308401.pdf.

422 Keith Bradsher, 'China Asks Other Nations Not to Release Its Air Data,' *New York Times*, 5 June 2012.

423 United Nations, *Vienna Convention on Diplomatic Relations* (Vienna: United Nations, 1961).

424 Jovan Kurbalija, 'Is tweeting a breach of diplomatic function?,' *DiploFoundation*, 14 June 2012.

425 Creating and maintaining a collective 'Who is who in cyberspace' directory across the government may be a solution to overcome this hurdle.

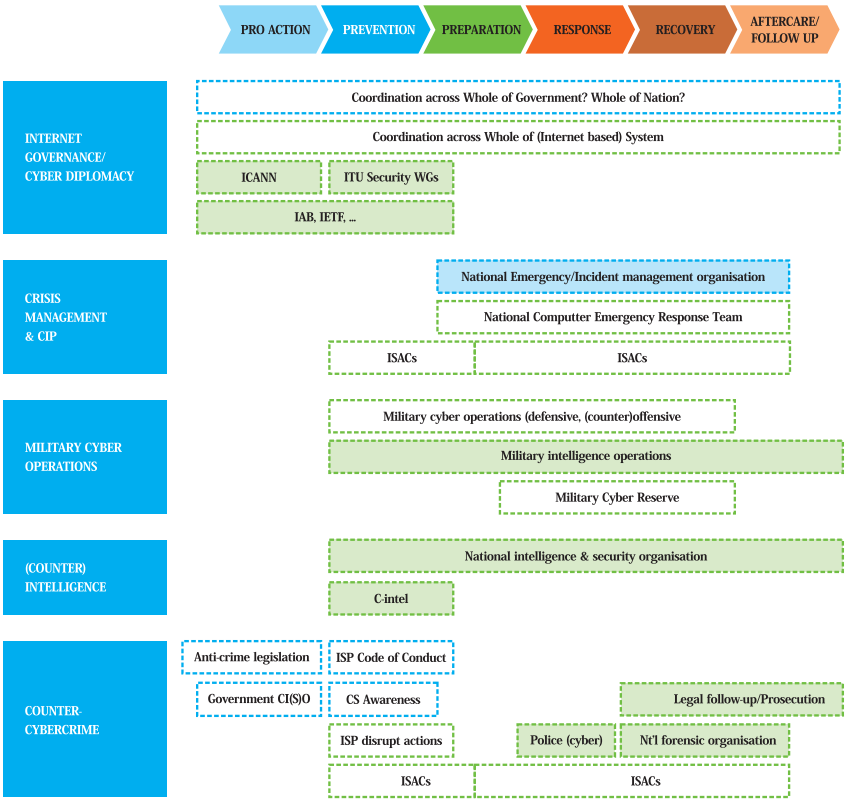

Figure 6: The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

4.6. THE THREE CROSS-MANDATES ACTIVITIES

Besides the five specific types or mandates of national cyber security, there are also activities that apply to each of these mandates. Figure 7 shows the position of the organisations along the elements of the incident management cycle. Furthermore, the often complex relationships with international organisational structures will only be touched upon here briefly. They will be explained at length in Section 4.7.

4.6.1. Coordination

The cyber security coordination cross-mandate function is also seen as constituting national governance for cyber security. The coordination crosses the mandates discussed in Section 4.5 and spans the strategic, policy, and operational/tactical levels on the one hand, and all six elements of the incident management cycle on the other one. For a proper understanding, it shall be noted that the coordination concerns the wider understanding of cyberspace (or all ICT) and not just the internet[426] – unless a nation has specifically restricted itself to internet-connected ICT only in its NCS strategy (NCSS).[427]

In contrast to many other national security domains, cyber security crosses most of the classical governmental mandates. This requires a pro-active governance function within the national government which coordinates and spans the Whole of Government approach (WoG) and the full spectrum of the cyber security incident management cycle. The coordination responsibility is often assigned to a department responsible for more cross-departmental and agencies coordination activities (e.g., like the Cabinet Office or similar head of government functions).

This function will have a number of central roles. These include the coordination of a NCS risk assessment; the development and maintenance of a NCSS,[428] the alignment with the critical (information) infrastructure protection strategy (C(I)IP), and the possible establishment of a national (public-private) cyber security council.[429] Optimally, the same group will also play a decisive role in crisis management and any foreign security incidents involving cyber. A National (public-private) Cyber Security Council is meant to focus on pro-action, providing a well-balanced advice at the strategic level on cyber security issues and trends. However, during a major cyber security incident, crisis management may ask guidance from the Council. For that reason, the box in Figure 6 extends along all elements of the cyber security incident management cycle.

If a nation has developed and politically agreed on a NCSS, then it should set the policy outlines for the WoG. Each individual department may then develop strategies and policies for their own mandate, subordinate to the national policy and strategy. Moreover, the NCSS shall align with other national strategies and

---

426 Includes, for instance, process control systems, medical equipment, in-car systems, or RFID-chips.

427 Nations which, according to their NCSS, use an internet-only understanding of cyberspace are: Australia, Canada, Germany, Spain and New Zealand.

428 Eric Luiijf et al., 'Ten National Cyber Security Strategies: a Comparison,' in *Critical Information Infrastructure Security*, ed. Bernhard M. Hämmerli and Stephen D. Wolthusen (Springer-Verlag, forthcoming).

429 For example: Eijndhoven, 'Dutch Cyber Security Council Now Operational.'

policies, and recognise internationally agreed and nationally ratified cyber security treaties, legislation and regulations (e.g., those set by the EU and the Council of Europe Cybercrime Convention[430]). Optimally, the coordination body would supervise these developments.

Although a nationally coordinated approach and an internationally harmonised NCS legal framework would be preferred, most nations split the specific function of 'creation and maintenance of legal framework and regulation' across the various departments involved. For example, specific cyber security legislation and regulation regarding the telecommunication sector lies with a ministry of communications or economic affairs, whereas counter cyber crime legislation is supervised by a ministry of justice (or the like). The military task of establishing standard operation procedures and rules of engagement within the cyber domain is often dealt with purely within the military domain, and is seldom carried outside – with the possible consequence that the foreign ministry and the military/intelligence community might have a very different idea of what is 'legal' in cyberspace.

The most obvious governmental organisation to look after the international cyber security arrangements is a ministry of foreign affairs. However, given the spread of functions and responsibilities across the governmental mandates, often a specific ministry such as the ministries of economic affairs, telecommunications or health takes the lead. To avoid conflicts between departments and to harmonise the nation-wide approach, the ministry of foreign affairs is preferably in charge of the external cyber security policy coordination function, and draws on the other departments to provide factual expertise.

At the operational/tactical level, the coordination department, the intelligence community, or an interior ministry will be in charge of providing cyber security to the WoG, often under the responsibility of the government Chief Information Officer (CIO) or Chief Information Security Officer (CISO) (also see Section 4.5.5). Activities may, for instance, include awareness building; procedures and regulation for dealing with national secrets; standardisation of open source resources, and provision of, or oversight to, a government-wide digital signature infrastructure.

A separate, very specific, organisational function in the cyber security domain is the capability for an independent review of major cyber security incidents at the national level. By adding or contracting the right level of cyber expertise, this function can be embedded within an existing national incident review capability (e.g., a national safety and security board).[431] An example of such a review is the lessons identified

---

430 Council of Europe, *Convention on Cybercrime (ETS No. 185)*.

431 See, for instance, The Dutch Safety Board, http://www.onderzoeksraad.nl/en.

study[432] about the Dutch DigiNotar case, where the digital certificate provider for the Dutch government, its agencies, towns and municipalities and a number of private companies, was compromised.

4.6.2. Information Exchange and Data Protection

Few activities are as central to national cyber security as information exchange and data protection. The information exchange and data protection cross-mandate has its main focus on prevention, response, and recovery. The cross-mandate is mainly of operational/tactical nature. However, tactical information exchanges will occur during preparation and aftercare/follow up by specific organisations, such as national crisis management organisations and investigation organisations respectively. Data protection may be a consideration at the political/policy and strategic levels when considering new laws and cyber functions for society.

Information exchange[433] on cyber security information builds upon trust and value between two or more organisations and, sometimes, is even limited to mutual trust between persons only. Information sharing should not be confused with information provisioning, where an organisation is required by law or its mandate to provide (processed) information one-way to other parties, subject to relevant data protection requirements. Key to information sharing is the two way value-adding exchange of information on cyber security while balancing transparency and secrecy. Globally, the information age requires a need-to-share recognition balanced with trust and tempered by the need-to-know paradigm of information assurance. Cyber security information to be shared may include weak signals, incident data, threats, risk, security measures, coordinated defensive responses, tactical/operational experiences and good practices.[434]

Information sharing takes place within national and international communities that have a specific objective within the same mandate. This can include information exchanges between communities in alike mandates in different nations; international exchanges such as the European SCADA Security Information Exchange (EuroSCSIE); the European Financial Services Information Security Analysis Centre (FS-ISAC), and the Club de Berne (intelligence community), or between different communities in different national and international mandates such as critical infrastructure operators, police, and intelligence and security services.

---

432 The Dutch Safety Board, The DigiNotar Incident: Why digital safety fails to attract enough attention from public administration, (The Hague: Dutch Safety Board, 2012), http://www.onderzoeksraad.nl/docs/rapporten/Rapport_Diginotar_EN_summary.pdf.

433 Klaver, Luiijf, and Nieuwenhuijs, *The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe.* 51-60.

434 Ibid., 52.

4.6.3. Research & Development and Education

Typically, nations envision economic prosperity from information and communication technologies in their NCSS.[435] Nations often assign their strategic/operational level responsibility for stimulating innovation and economic development of cyber security R&D to their ministry of economic affairs. The strategic/operational management level aspects of the academic, often more fundamental, cyber security research efforts are managed by a ministry of science/education, in a number of cases in close coordination with a ministry of economic affairs and the more security-orientated ministries. The actual R&D programmes are managed at the tactical/operational level either by existing national organisations which manage R&D programmes in a wide set of research domains, such as companies or universities, or by specifically established organisations. A specific, academic-based organisation may be established which assists in the analysis and identification of lessons about the government response to a major cyber crisis.

By nature, R&D efforts are often prevention activities. This is notwithstanding the fact that these efforts include the R&D on support methodologies and measures for the preparation, response and recovery elements of the cyber security crisis management, military cyber operations, and counter cyber crime mandates. It can also include in-depth research into cyber attacks and their consequences that could potentially be used in more offensive activities.

Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education. A nation requires its ministry of education and/or science to develop strategic/operational programmes for cyber security awareness and education. The base level programmes need to span a wide range of stakeholders: children at primary and secondary school, and a base level of awareness for adults and elderly people. Some of these programmes, however, may be organised and paid for by private industry (e.g., an anti-phishing TV campaign by financial institutions). It is, however, beneficial at the national level to orchestrate operational activities in order to avoid the duplication of efforts.

Apart from the general population and specific target groups within the population, a cyber security educational structure is required to assure that a sufficient number of cyber security experts and professionals are educated (and re-educated) to support all the cyber security activities outlined above, as well as in organisations outside the critical sectors and government.

At least as important as basic education is awareness raising among key decision-makers in both state and non-state organisations as to the extent of the cyber

[435] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies.'

security challenge. This is particularly acute as the complexity and sometimes esoteric nature of the subject prevents a 'natural' education of these decision-makers over time. At the same time, the plurality of actors in cyber security means that especially the cooperation of non-state decision-makers is absolutely crucial in any NCSS – and this cooperation often will only occur when those decision-makers are fully aware of the extent of the challenge.

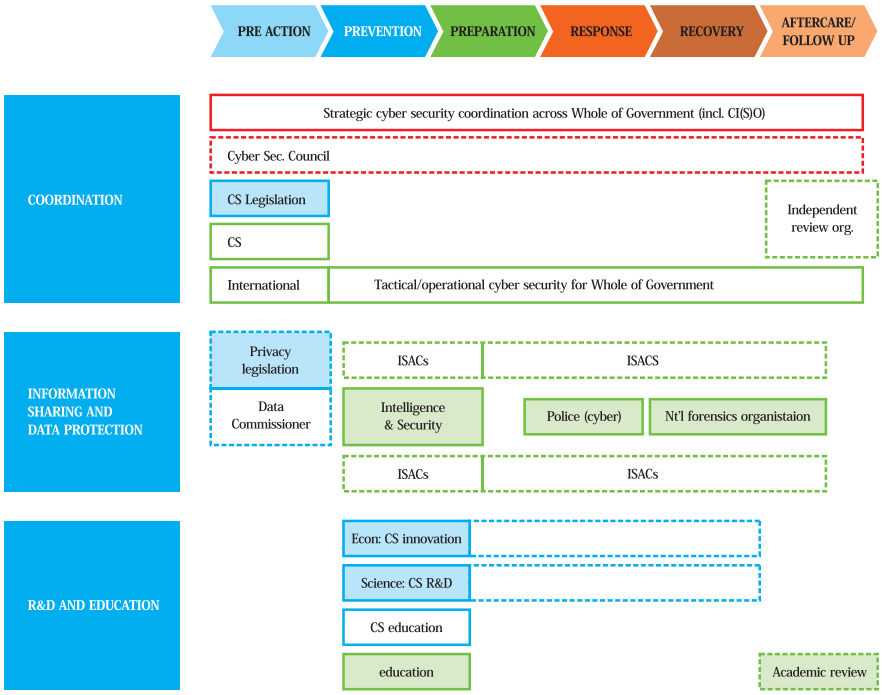

Figure 7: The Organisational Picture of the Cross-Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

4.7. INTERNATIONAL CYBER SECURITY ORGANISATIONS

International organisations play a key role in cyber security, although they often only receive passing mention in NCSS. These NCSS will highlight the importance of international cooperation, and mention a few of the most prominent international organisations but often with a lack of detail of how or why these organisations are

important. First and foremost, NCSS deal with the international spectrum primarily as a WoG and, to a lesser extent, as a Whole of Nation (WoN) matter. Whole of System (WoS) approaches, when not government focused (such as within an international organisation), are much more difficult for national governments to conceptually deal with. These groups however represent a good share of international cyber security activity (in particular at the technical/operational level), which means that government consistently has trouble engaging to its full potential.

4.7.1. Government-Focused Activities

As mentioned earlier, the Whole of Government approach (also known in the UK as 'joined-up government' and the US as 'networked government') was originated to save costs and improve coordination. When discussing international organisations, WoG is being used here to discuss international cooperation between governments that generally exclude the private sector or civil society. These organisations tend to focus on the internet governance and cyber diplomacy, although much more emphasis is laid on the latter than the former.

The governments of the United States, Japan and the United Kingdom provide good examples of organisations which coordinate all international aspects of cyber security. The US has an appointed US Cyber Coordinator (in the White House National Security Staff), Japan has its own National Information Security Center and the UK has established the Office of Cyber Security and Information Assurance (with the two latter organisations being attached to their respective Cabinet Offices). These offices have senior people in (generally) sufficient numbers to coordinate other government ministries and departments. Often, the members of these offices are actual detailees seconded from those ministries, which aids speedy coordination. For instance, the UK International Cyber Policy Unit (ICPU) is located within the Foreign and Commonwealth Office but is largely staffed with individuals 'double-hatted' from the Cabinet Office. While the ministries of foreign affairs will have the functional lead, these central coordination groups have a strong role to play. In the United States, for instance, it was the National Security Staff, not the State Department, which led the writing and coordination of the International Strategy for Cyberspace.

WoG international activity solutions are often concentrated within bilateral agreements (i.e., cyber diplomacy), although there is a growing number of engagements inside intergovernmental forums. Bilaterally, there have been several important recent agreements. For example, India has signed cyber security

agreements with both the United States[436] and Japan.[437] To extend the extensive cyber security partnerships of the USA and the UK, the White House announced early 2012 that, 'President Obama and Prime Minister Cameron reaffirmed the vital partnership between [their] two nations on cybersecurity,'[438] and enumerated six specific areas of progress.

State to state agreements (outside of larger multilateral groupings) were originally relatively rare but, are rapidly increasing as an option for states,[439] such as when 'the United States and the United Kingdom [...] launched a trilateral initiative with Australia to fund new R&D for improved cybersecurity.'[440] Some agreements also already exist to facilitate cyber crisis management cooperation: a good example for this is the 'China-Japan-Korea (CJK) agreement.'[441]

These bilateral and multilateral agreements typically do not lead to the creation of new organisations to shepherd the agreed upon actions. They rather lead to increased cooperation between existing organisations, especially CERTs and ministries of defence and justice/the interior.

Cyber security agreements through intergovernmental organisations rely on the existing staff and bureaucracies of those groups. The most important tend to be long standing groups created to coordinate traditional national security and diplomatic issues. In 2012, the United Nations will be hosting the third meeting of the Group of Government Experts (GGE), organised by the Office of Disarmament Affairs, to discuss cyber norms.[442] China, Russia and other nations have issued a draft Code of Conduct calling for cyber norms, based on work done previously with the Shanghai Cooperation Organisation.[443] Meanwhile, the UN's ITU is often perceived to be striving to 'wrest control' over the internet from ICANN.[444]

Cyber issues have been on the NATO agenda for some time. Unlike other international organisations, this military alliance has extensive cyber systems which need to

---

436 US Department of Homeland Security, 'United States and India Sign Cybersecurity Agreement,' *Office of the Press Secretary*, 19 July 2011.

437 TNN, 'India and Japan agree to boost maritime, cyber security,' *The Times of India*, 1 May 2012.

438 White House, 'Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace,' *Office of the Press Secretary*, 14 March 2012.

439 See Section 5.3. for a discussion on non-NATO nation cooperation.

440 White House, 'Joint Fact Sheet: U.S.-UK Progress Towards a Freer and More Secure Cyberspace.'

441 English.news.cn, 'China, ROK, Japan pledge future-oriented partnership amid trilateral summit: joint declaration,' *English.news.cn*, 14 May 2012.

442 UNODA, 'Developments in the field of information and telecommunications in the context of international security,' United Nations, http://www.un.org/disarmament/topics/informationsecurity.

443 Jason Healey, 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms,' *New Atlanticist*, 21 September 2011.

444 See for instance http://www.bbc.com/news/technology-19106420.

interconnect with its many members during military operations. Accordingly, most of NATO's recent initiatives have been aimed at improving the cyber security posture of its own systems and it has a more pronounced focus on the mandate for military cyber defence operations than other international groups.[445]

There are some other international groupings that are customised just to deal with cyber (and other information protection) issues. Meridian is perhaps the most well-known. Since 2006, a programme committee comprised of international governmental organisations organises the annual event and develops the agenda (such as the Department of Homeland Security of the United States or the Infocomm Development Authority of Singapore).[446]

4.7.2. Nation-Focused Activities

The Whole of Nation approach, as mentioned earlier, includes a mix of government, private sector and civil society. Compared to government and internationally-focused organisation, WoN groups are the least difficult to categorise in the international sphere, although these non-governmental actors account for the bulk of what is termed 'national' cyber security, with a heavy focus on the mandates of crisis management and CIP. In international cyber security, WoN is used to describe where governments work closely with non-government groups, while still retaining a substantial voice, such as within the 'Organisation of Islamic Cooperation – Computer Emergency Response Team' (OIC-CERT).

The OIC-CERT is a grouping of organisations from Islamic nations to 'explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cyber security.'[447] While it is open to membership from academia, companies and individuals, the group reserves full membership (and voting rights) only to governments.

A completely different example comes from recent collaborative *ad hoc* actions against networks of malicious computers called botnets. These 'take downs' were led by companies in the private sector but relied upon the coercive power of national justice systems. Microsoft has become especially well known for using this innovative tactic: teaming with other companies with knowledge of a particularly vicious (or vulnerable) botnet and then filing suit in court against the botnet's organisers. Using this authority, Microsoft and its partners, 'escorted by the U.S. Marshals – successfully executed a coordinated physical seizure of command and

---

445 Jason Healey and Leendert van Bochoven, 'NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow,' *Atlantic Council Issue Brief*, February 2012.

446 Meridian, 'The Meridian Process,' Meridian 2007, http://www.meridian2007.org.

447 OIC-CERT, 'Mission Statement' OIC-CERT, www.oic-cert.net.

control servers in two hosting locations to seize and preserve valuable data and virtual evidence from the botnets for the case.'[448]

4.7.3. System-Focused Activities

In the Whole of System approach there is cooperation among 'like-minded actors.' The government does not necessarily have any privileged position in the group. As in WoN, these WoS groups tend to keep a heavy focus on the mandates of counter cyber crime, crisis management and CIP. Despite the wide scope for effective and agile action of these non-state groups, they are often overlooked by NCSS.

One of the most important WoS organisations has already been discussed earlier. ICANN embraces a multi-stakeholder approach, so governments have a voice, but so do technical experts from the private sector and civil society.

The importance of WoS groups cannot be overestimated. For example, during the 2007 cyber attacks against Estonia, private sector members of NSP-SEC (Network Service Provider Security), a leading cyber attack mitigation coordination body of internet network professionals 'went to the EE-CERT [the Estonian CERT] to act as the liaison and to help the [Estonian] EE-CERT coordinate with CERTs and internet service providers in other countries to stem the attacks.'[449] The support for Estonia came not from NATO or other governments but through a non-governmental group.

Getting vetted into NSP-SEC is especially difficult as, once you are in, you have a positive obligation to stop any attack traffic traversing your network as soon as you are notified by another member of the group, no questions asked. As Bill Woodcock summarised it: 'If something needs to be taken down, it needs to be taken down and there isn't time for argument and that's understood up front, so there isn't a mechanism for arguing about it. You can argue about it later.'[450]

While NSP-SEC only operates in the phase of incident response, there are numerous other groups that cover other parts of the spectrum. For example, since 1990, the Forum of Incident Response and Security Teams (FIRST) has been 'an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.'[451] As with NSP-SEC, governments are members but have no privileged status.

---

448 Jeffrey Meisner, 'Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets,' *The Official Microsoft Blog*, 25 March 2012.

449 Jason Healey et al., Building a Secure Cyber Future: Attacks on Estonia, Five Years On [Transcript], (Washington, DC: Atlantic Council, 2012), http://www.acus.org/event/building-secure-cyber-future-attacks-estonia-five-years/transcript.

450 Ibid.

451 FIRST, 'FIRST Vision and Mission Statement,' FIRST, http://www.first.org/about/mission.

FIRST is one of the founding blocks of the CERT community.[452] Derived directly from the first worldwide CERTs and managed from a university, FIRST is essentially the most important certification body for any organisation or government seeking to be part of the worldwide CERT community. Members are able to collaborate with like-minded members across the entire spectrum of cyber security actions. FIRST working groups develop a whole range of tools, processes and products which are usually freely available.[453]

NSP-SEC and FIRST are long-standing groups, but other WoS organisations are *ad hoc* creations for a single purpose. Also known as 'Security Trust Networks',[454] these groups are often volunteer based, and concentrate a lot of operational or research capability within a completely informal network. Led by Microsoft, the Conficker Working Group was 'a collaborative effort with technology industry leaders and academia to implement a coordinated, global approach to combating the Conficker worm,' a particularly virulent piece of malicious software.[455] Even though these like-minded groups are at the forefront of much of cyber security, especially incident response, governments typically have little understanding of them or how to aid or even make room for them. For example, after battling Conficker, members of the working group said they' saw little participation from the government,' indeed even 'zero involvement, zero activity, zero knowledge.'[456]

There are, of course, active government-only international cyber security groups (e.g., the European Government CERT Group is a vital organisation within European cyber security), but most international cyber security groups are still non-state. Recognising the importance of these WoN and WoS groups in NCSS is an important step to improving security. Understanding the importance of non-state groups is, however, absolutely essential.

---

452 Bruce et al., *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (TNO Report 33680)*. 77-80.

453 FIRST, 'FIRST Vision and Mission Statement.'

454 Klimburg, 'Whole-of-Nation Cyber Security.'

455 Conficker Working Group, 'Announcement of Working Group,' Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ#toc6.

456 The Rendon Group, Conficker Working Group: Lessons Learned, (Washington, DC: Conficker Working Group, 2011), http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf. 34.

4.8. ORGANISATIONAL PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

As some nations concentrate their cyber security on internet-connected systems only, a wide open gate is left for cyber crime in the other parts of cyberspace. A wide organisational understanding of cyberspace is needed to avoid organisational failure at the national level.

Leaving a policy vacuum: one pitfall is that nations unintentionally may leave a strategic and/or operational level vacuum around tactical capabilities – in other words, may create a 'labelled' department bereft of basic expertise or tasks, and without a top-level strategic vision. This vacuum will progressively fill itself due to function creep both vertically and horizontally,[457] leading to friction with other public and private organisations, and could also lack proper accountability.

Allowing stovepipes: cyber security is a global issue which crosses all governmental mandates, departments and agencies. There are many chances for the departments to engage in 'cyber empire building', using 'stovepiped' domains such as telecommunications, security, energy, health and economic innovation to overtly focus resources, legislation and regulations – detrimental to the exclusion of other issues. Moreover, the bureaucratic reality is that, in most nations, the cyber security subject areas are kept separate from each other in distinct mandates, often with their own definitions, emphasis and official slang.[458] The risk is very high that a strong stovepiped approach will lead to a set of uncoordinated, even overlapping activities and miscommunication. It will confuse private organisations which are faced with conflicting laws and regulation. For instance, cyber security breach notification obligations may be in conflict with privacy legislation, financial oversight or stock exchange rules. A strong coordination across the Whole of Government and strong public-private arrangements may help to avoid that situation. Even better is to link existing organisational structures together in a matrix structure – an effective and efficient way of building connectivity across governmental 'stovepipes', across public-private partnerships, and across trans-border networks.

Drafting obsolete legislation: another pitfall noticed in many of the current NCS approaches, is the organisational lack of governmental structures to prepare for new cyber threats and new ICT innovations. The rate of change in cyberspace means that organisations are constantly challanged by the need to modfiy

---

457 An incident response function like a CERT shall be focused on incident response and recovery. Some form of preparation is required. However, when such a CERT lacks a proper strategic/operational embedding, function creep may occur towards, for instance, pro-action and prevention aspects of critical infrastructure protection, and the area of cyber security policy development for its constituency.

458 See Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65).*

stovepiped services and legislation.[459] As a result, cyber security legislation covers the digital crimes known from the past and do not embrace new ones. In particular, fundamental elements of cyber security – especially the need to concentrate on the obligation of the defender to adequately secure his systems rather than only trying to pursue a most often unknown attacker – have often not been appreciated by lawmakers.

Lack of flexible cooperation: apart from the WoG angle, new non-state organisations are constantly emerging whose work is relevant to NCS. Either in prevention or in the response/recovery/follow up phases, these new organisations often deal with cyber security issues in a bottom-up mode. They often find their existence in new types of community arrangements with minimum or even no government influence. The ability to flexibly work with these non-state organisations is thus an important part of future national cyber security.

Unclear Information Exchanges: when it comes to information exchange, unfortunately, many governments just know they want it. However, often they only have little knowledge about the actual goal of sharing or coordinating information between departments, let alone with international and/or non-state actors. Accordingly, companies in one CIP sector may get overlapping or competing requests to share information from ministries of the interior, justice or defence, from military services or commands, as well as functional ministries (such as financial regulators) and a cabinet office. This threatens to undermine the entire purpose of an information exchange, and can make a critical operational function into an organisational burden.

Tolerating Cyber-Illiteracy: another gap identified is the understanding of cyber security issues and 'language' by higher level public officials, decision-makers, judges and politicians. No standard and base level education training has been identified for those key individuals. The lack thereof causes misunderstanding, adverse decision-taking, imbalanced sentencing, and neglect of serious threats and incidents.

[459] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies,' 23.

Internet Governance and Cyber Diplomacy

The UK Foreign and Commonwealth Office (FCO) was one of the first foreign ministries to dedicate staff to coordinating and addressing the international aspects of cyber issues. Previously under the auspices of the FCO Director for Intelligence and National Security, the FCO dedicated resources from 2011, building up to a full team in 2012, in the newly-formed International Cyber Policy Unit (ICPU). ICPU staff are either from the FCO or the Cabinet Office for Cyber Security and Information Assurance (OCSIA). Its Director is double-hatted for FCO and the Cabinet Office. The ICPU is well-resourced – relatively speaking, no other NATO nation has committed a similar level of staffing to addressing international cyber issues. It leads and coordinates the UK engagement on international, multilateral and bilateral cyber diplomacy issues. These range from discussions on confidence building measures and norms of state behaviour to the economic and social benefits of cyberspace, while bilateral issues can also include transparency building to various degrees of operational cooperation.

ICPU works closely with the full range of UK government departments engaged in cyber issues from UK Department on Culture Media and Sport on internet governance issues, to the Home Office on cyber crime. Within the international multi-stakeholder context, ICPU has the oversight of the UK government position and supports other government departments where these are in the lead. Each UK government department has its own well defined role to play but OCSIA takes responsibility for ensuring delivery of the national cyber security strategy through coordinating government policy on cyber.

Crisis Management and Critical Infrastructure Protection

The *Centre Opérationnel de la Sécurité des Systèmes d'Information* (COSSI) is the primary cyber defence organisation of the French government, and operationally responsible for managing national cyber crisis incidents. As part of ANSSI (a dedicated agency responsible for government information security within the Defence and National Security Department), COSSI is responsible for collating intelligence related to cyber threats both for the French government as well as for some of the critical infrastructure providers. COSSI is responsible for implementing many of the regulations and emergency ordinances of PIRANET, the French national cyber crisis management plan. In this context, COSSI depends mostly on CEVECS, a situational analysis and early warning centre that draws data from a wide array of feeds, and which has a 24/7 watch & warning component. The technical component of COSSI is mostly met by CERTA, the French government CERT, which receives technical alert information through a number of systems. At higher PIRANET alert levels, CERTA and CEVECS can be substantially reinforced with other personnel from the national security and defence ministry..

Military Cyber Operations

The US military was probably one the very first militaries to have cyber units. The first such unit was the 609th Information Warfare Squadron of the US Air Force, which was stood up in 1996. The unit had both offensive and defensive capabilities that were to directly able to support combat operations.[460] In 1998 the Department of Defense (DoD) created the first joint cyber command – commanded by a two-star general – with the authority to order, rather than just coordinate, military defences. Within two years, the Joint Task Force on Computer Network Defense (JTF-CND) was also assigned the cyber offense mission, although this was re-assigned to another command a few years later when the JTF was given authority over, not just global network defence, but operations as well.[461] JTF-CND retained this responsibility until 2010.

In the intermediate period, a great number of cyber organisations proliferated across the DoD and the US National Security Agency (NSA – a DoD subordinate agency). It was to streamline all these various organisations into one command that the US Cyber Command (USCYBERCOM) was stood-up in 2010. As a major shake-up of the US military in cyber, USCYBERCOM was designed to overcome a large number of 'stovepiped' conflicts within the DoD. Henceforth, the activities of all four branches of the armed forces would be communicated, coordinated and, in part, directly controlled by USCYBERCOM. As a subordinate of US Strategic Command, USCYBERCOM is also the top-level organisation with final responsibility for DoD-related cyber offensive and defensive activity. A major novelty of USCYBERCOM was its collocation within the NSA and the 'double hatting' of its commander as also the director of the NSA. Besides the obvious resource benefits that this relationship provided, it also addressed a number of significant operational concerns, particularly with regard to the difference between espionage and warfare. In 2011, the official USCYBERCOM budget was over $3.2 billion, but this did not take into account supporting budgets within the NSA or other aligned structures and commands.

460 Jason Healey and Karl Grindal, 'Lessons from the First Cyber Commanders,' *New Atlanticist*, 14 March 2012.

461 Ibid.

Intelligence and counter-intelligence

Sweden maintains one of the most advanced Signal Intelligence (SIGINT) systems in Europe, operated by the National Defence Radio Establishment (FRA). With wide authority to tap foreign voice and data communications crossing its territory, FRA also operates under very close (and very transparent) supervision by specially appointed legal bodies. No data inspection may be conducted by the FRA without a specific request being issued by the Swedish Defence Intelligence Court – a body specially set up 2009 to protect 'personal integrity' in cases of surveillance. The Court also controls the search criteria and other provisions to limit the amount of accidental surveillance that may occur, and an independent 'Integrity Ombudsman' further shadows the work of the Court. Institutional oversight of the Court itself is provided by a separate judicial body, SIUN, which is also able to directly investigate intelligence activities of the Armed Forces. SIUN can also initiate investigations upon request of private persons.

Counter Cyber Crime

Brazil has been confronted with one of the fastest growing local cyber crime populations in the world. Increasingly, these cyber criminals are not only internationally active, but also pose a serious threat to Brazilian internet users as well. Consequently, in recent years the Brazilian Federal Police has greatly invested in counter cyber-crime resources, increasing both the ability to undertake network investigations as well as conduct (hardware) forensic analysis. Two units were especially emphasised – the centralised Cybercrime Suppression Unit (URCC), and the Computer Forensics Unit (CFU). The forensic specialists are particularly intended to support investigations of the URCC by being able to quickly and reliably respond to local investigations across the territory of Brazil. The CFU, which has been active since 1996, has a headquarters unit with around 24 specialists, but mostly operates through some 180 forensic specialists in about 50 field offices. A highly flexible pay structure has allowed the Federal Police to offer forensic specialists and others very high salaries, leading to a high standard of recruitment.