This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

RAND EUROPE

Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)

Unclassified Summary

Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune,
Alain Esterle, Pablo Rodriguez

Prepared for the European Defence Agency

The research described in this document was prepared for the European Defence Agency.

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

This document is an unclassified summary report of the study into military cyber defence capabilities produced for the European Defence Agency (EDA).

Cyber defence was identified as a priority by the participating Member States (pMS) in the Capability Development Plan of 2010, alongside a number of other areas for capability development (such as network enabled capability). As a primary step, this Capability Development Plan identified an action in 2011 to: "Conduct a stocktaking exercise of capacities including concepts in the area of Cyber Defence being taken forward by EDA participating Member States, EU and NATO."

This is an unclassified summary of the main output of the study. Accompanying the classified Final Report at the EU RESTRICTED/UE RESTRIENT level are a set of Profiles for each Member State from the EDA's Cyber Defence Project Team (CD PT) participating in the research, setting their own maturity alongside that of the overall EU-level 'benchmark' presented in this summary.

This unclassified summary should also be read in the context of the EU's recent Cyber Security Strategy released in February 2013, which was finalised and published after this study was undertaken in 2012.

For more information about this study or this report, please contact:

Neil Robinson
Research Leader
RAND Europe (Brussels)
82 Rue de la Loi
B-1000 Brussels
Belgium
Tel : +44 (0)1223 353329
Email: neilr@rand.org
Web: www.randeurope.org/cyber

Alain Esterle
Chercheur Associé à la Fondation pour la Recherche Stratégique
Fondation pour la Recherche Stratégique
27 Rue Damesme
75013 Paris
France
Tel : +33 1 43 13 77 75
Email: a.esterle@frstrategie.org
Web: www.frstrategie.org

Summary

RAND Europe and Fondation pour la Recherche Stratégique were asked by the European Defence Agency (EDA) to undertake a stocktaking exercise of military cyber defence capabilities across the EDA's participating Member States (pMS). In the context of cyber defence, this has been accorded one of the top ten priorities by pMS in the EDA Capability Development Plan in 2010.

This exercise should not be understood as outlining plans for the 'militarisation of cyberspace'. However, in common with other organisations that use cyberspace the military has a responsibility to protect its own networks within its purview to deliver agreed strategic security goals. In the context of participating in EU common security and defence policy missions, the armed forces of EU Member States also operate under the principle that a risk accepted by one is accepted by all: a formulation of the common security principle that 'you are only as secure as your weakest link'. With the multifaceted nature of cyberspace, this is all the more important to consider.

In addition, this document seeks to lift the veil on these more 'exotic' forms of military capability and engender a spirit of trusted collaboration between member states.

Cyberspace is important, and is susceptible to a range of security risks

Concurrent with the increasing importance of cyberspace, a wealth of risks have emerged which, many argue, serve to jeopardise the achievement of benefits that cyberspace can offer.

According to the World Economic Forum, in its survey of key business leaders and governmental decision makers across the globe, cyber-security was regarded as one of the pre-eminent risks posed to modern socio-economic well-being. These risks stem from a range of factors, two key issues being:

- First, insure system and software development and implementation mean that vulnerabilities exist, and can be exploited by a wide variety of actors motivated by different reasons.
- Second, there are systematic properties of cyberspace which are driven by its complexity and are difficult to understand fully; not least because many are emergent. These include vulnerabilities that cannot be discerned yet, and complex cascading failures which arise due to the 'network of networks' paradigm which characterises cyberspace.

However, vulnerabilities are not only of a technical nature; socio-economic behaviour from a number of parties also can drive vulnerability in systems. This can be seen in the low priority that security is given in software design, and the seemingly risky behaviour adopted by individuals and organisations when it comes to some cyber-security practices.

Concerning threats, these are motivated from several directions including nation-states, intelligence agencies, proxies, serious and organised criminals and non-state actors. It is the multi-polar nature of these threats that provides policymakers with difficulty in marshalling the most appropriate response.

First, the potential to gain economic value is attractive to criminals. This is particularly the case as industrial players seek to capitalise on personal data, but also in the way in which cyberspace is the medium for commerce and trade. This has arisen to the extent that many countries regard serious and organised cybercrime to be a clear and present national security issue.

Second, there are also serious national security threats (which form the main subject of the full report): these include adversaries that seek to disrupt target nation-states' reliance on cyberspace. It could be via different means, including obtaining military secrets to provide for strategic, operational or tactical military advantage, or conducting operations to disrupt, destroy or interfere with military equipment, assets and infrastructure.

Finally, there are non-state actors who are not motivated by economic reasons, notably activists who may indulge in certain activities in cyberspace to bring attention to a particular cause.

The armed forces are reliant on cyberspace both as a user and as a domain to achieve defence and security missions

The role of the military in defending against these risks has yet to be fully defined and understood. Like any other governmental organisation, the military forces are increasingly reliant on cyberspace and this reliance creates specific risks, as they have a unique role as a state-sanctioned entity authorised to apply the use of force to compel adversaries. However, as cyberspace becomes such an important asset that its (in)security is now a national security concern, a question is raised as to what extent can force be used by military forces in defending this new domain.

This study sought to establish a better understanding of European cyber defence capabilities

The objective of this study was to establish a high level understanding of cyber defence capabilities across EDA pMS to support progress toward a more consistent level of cyber defence capability across the EU. Specifically, the study aimed to inform further action at the EU and national level.

This stocktaking exercise included research into the different EU level organisations involved in cyber-defence activities in the context of CSDP missions as well as data collection on cyber defence capabilities in each Member State. This was accomplished according to a common capability framework (described in the Appendix to this summary). The research was carried out via document review, semi-structured interviews and the development of a questionnaire distributed to those EU Member States participating in the EDA's Cyber Defence Project Team.

Cyber defence capability information was analysed according to a commonly understood military framework of functional contributors to defence capability, known as Defence Lines of Development (DLoDs). These contributors are Doctrine; Organisation; Training; Materiel;

Leadership; Facilities and Interoperability. Each country was qualitatively assessed in each contributor against a weighted maturity model.

pMS received a country specific report indicating their maturity against the EU modal average. An important outcome is the use of these profiles to help pMS prioritise capability development through learning from the experience of other countries. The EDA brokered information requests between pMS to maintain anonymity of responses.

Findings

Our research finds a complex and diverse picture with regard to cyber defence capability at both the EU level and within the pMS.

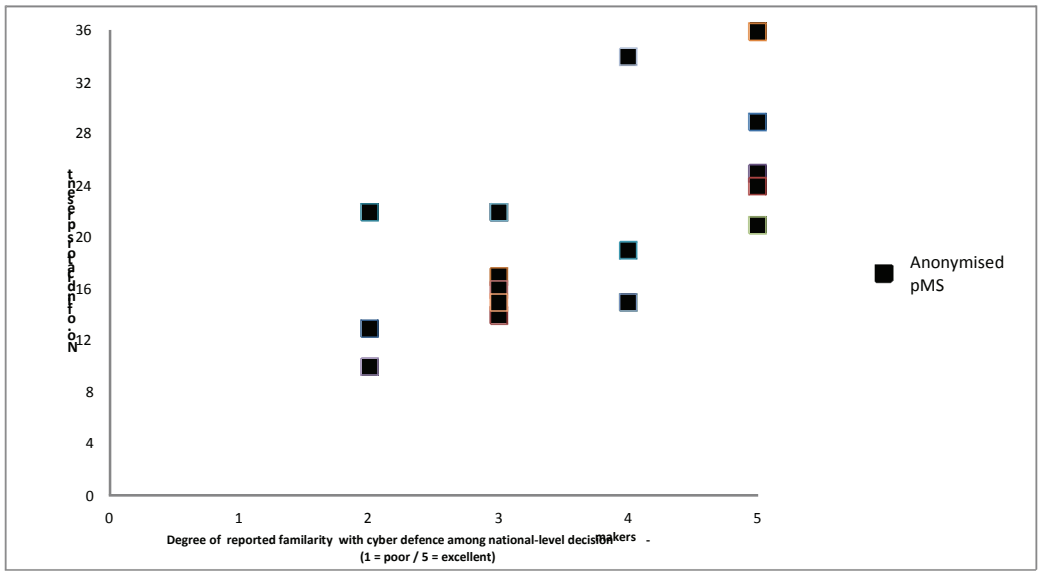
Findings at the EU level

Amongst relevant EU level organisations, we find a somewhat diverse picture with respect to cyber-defence. There is a complex operational setup regarding who undertakes cyber defence activities (e.g. detection; reaction; response) between the EEAS, General Secretariat of the EU Council and European Commission. Threat analysis & cyber-intelligence gathering capability appears to be emergent. Incident response capabilities could be deepened (especially given the deployed nature of some assets involved in EU-led CSDP operations). The culture of cyber-security good practice needs to be nurtured. The use of military specific standards and tools is still poorly understood. Finally, both NATO and the EU are pursuing similar activities in this area (albeit under different assumptions and limitations).

There is a mixed picture with respect to military cyber defence capability across participating Member States

Figure E.1 indicates the extent of presence of reported indicators relating to cyber defence capability against the reported familiarity of cyber security awareness among key decision-makers. It portrays a broad relationship between familiarity with cyber defence topics at a senior level and the extent of cyber defence indicators per country.

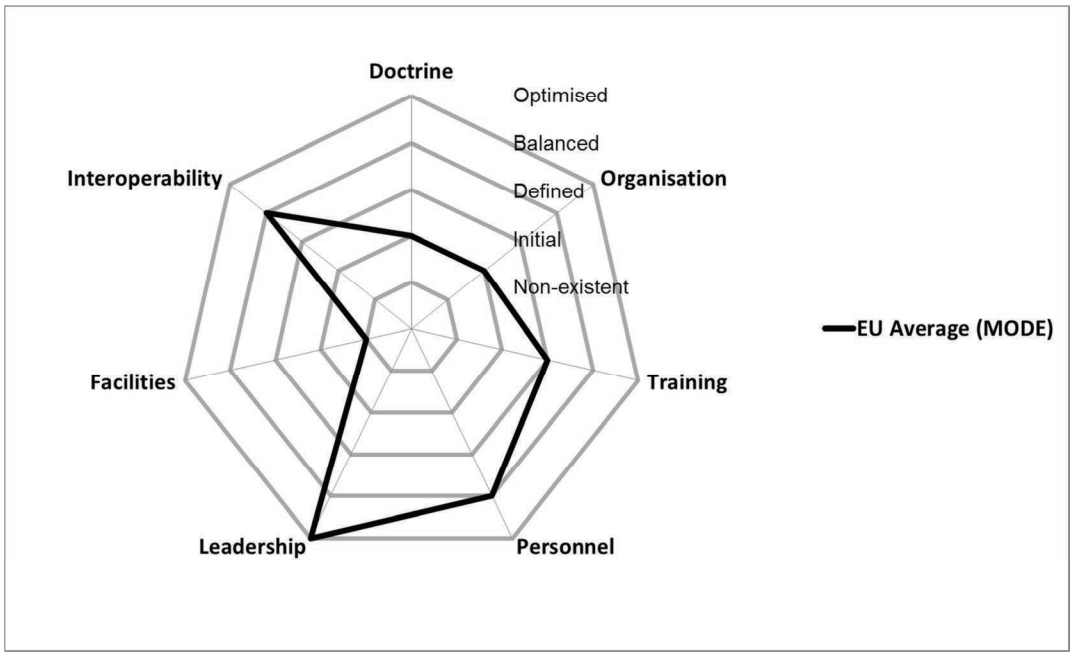
Figure E.1: Number of indicators compared to reported level of familiarity of senior military decision makers concerning cyber defence issues



It is encouraging that no country reported a 'poor' level of familiarity regarding cyber defence issues among its key military decision makers.

Figure E.2 indicates the EU average (mode – the most frequently-occurring observation) across most of the capability domains for 20 pMS.[1]

Figure E.2: Overall view of modal average of cyber defence capability across the European Defence Agency Cyber Defence Project Team participating Member States



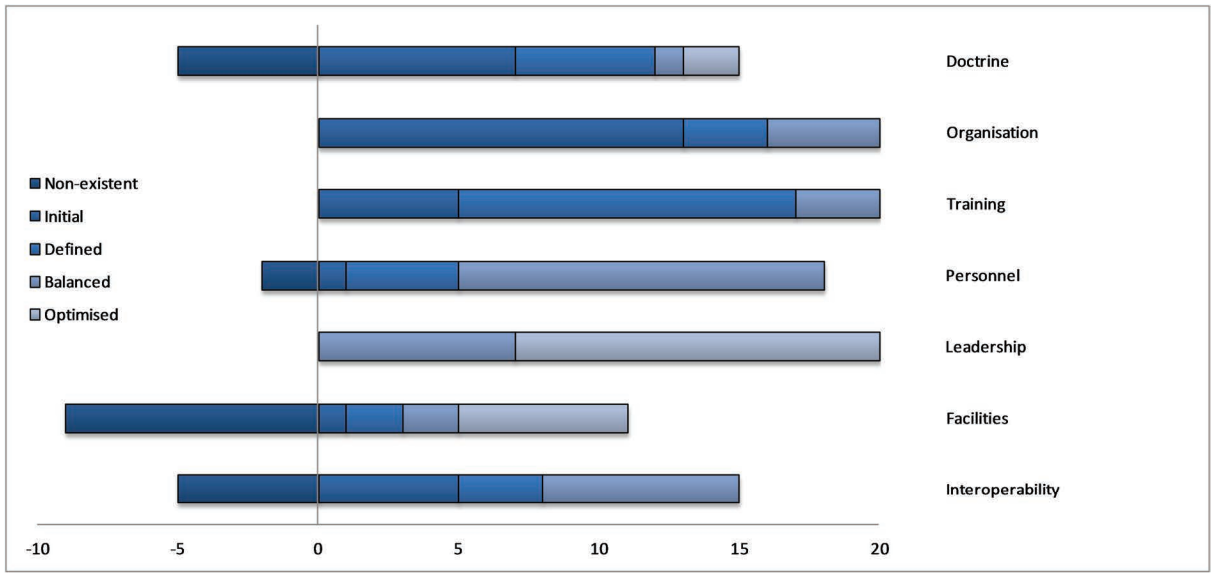
- The 20 pMS exhibit strengths (in the context of our weighted maturity model) in three capability domains. Regarding the capability domain of *Leadership* (which covers the existence of and clarity concerning escalation mechanisms for national-level cyber defence incidents), most participants were at Optimised. Given the incident response-related nature of many cyber defence units, perhaps this is unsurprising. Under *Personnel* (a category that covers personnel management, vetting and recruitment and retention policies) and *Interoperability* (a category covering the existence of enterprise interoperability frameworks – schema to support information flow across defence organisations and wider public administration), the pMS modal average was Balanced. Perhaps this also comes as no surprise. Militaries might be regarded as being more culturally attuned to personnel management issues through well-established concepts of operational security and a legacy of handling protectively marked information.
- For both *Doctrine* and *Organisation* most pMS remain at an early level of maturity, according to our model. Concerning *Training*, we find a slightly more mature situation. It is clear that out of the three capability areas of Doctrine, Organisation and Training, pMS are more mature with respect to *Training* (training mechanisms at both working and executive decision maker level; participation in exercises, etc), than the more complex and longer-term efforts required to establish organisational structures and mandates to and negotiate and agree strategies, doctrine and concepts. This is despite our weighing the three areas of *Doctrine*, *Organisation* and *Training* as equally 'hard' in which to achieve progress toward maturity.

[1] Data on Materiel and Logistics is excluded, as only 11 countries provided data on this aspect.

- The domain of *Facilities* (eg specific physical infrastructure dedicated to cyber defence missions such as laboratories, test facilities, and so on) stands out as highly immature (Non-Existent).

Figure E.3 presents the frequency of maturity levels across the 20 pMS included in this analysis. This illustrates how many pMS are in each maturity category. The count of countries analysed as having non-existent maturity for each capability area is shown to the left of the axis going through zero. The various levels of existing capabilities (Initial to Optimised) are depicted on the right side of the scale.

Figure E.3: Frequency of maturity levels per capability domain



As can be seen in Figure E.3, the picture is slightly more complex when we consider the frequency (ie numbers of countries) of each level of maturity in each of the capability domains. Figure E.3 is better understood as being used to inform an assessment of an EU minimum (assuming an Initial level of maturity as just such a baseline). For example, although in the domain of *Doctrine* most countries are at an Initial level of capability, there remain a number of countries that possess a non-existent level of maturity.

The capability domain where there is most left to be done is *Facilities* (ten countries below the Initial level of maturity) and *Interoperability* (five countries below the Initial level of maturity). *Leadership* is perhaps the most advanced, with many countries at either the M4 Balanced or M5 Optimised levels. Under the capability domain of *Organisation*, every country is at least at an initial level of maturity, which may be regarded as positive. At the same time, the majority of countries are at an Initial level. This suggests that further work might be necessary with respect to supporting pMS in developing organisational capabilities. The picture is only slightly better for *Training*, where a majority of countries are at level 3: Defined, suggesting that there is plenty of further work which can be done in this domain.

Recommendations

Our recommendations are aimed at both EU level stakeholders and toward senior policy-makers in pMS.

Recommendations at EU level

Building on the consultations and evidence from the EU-level stakeholders, we propose a number of discrete avenues for EU institutions to consider, summarised below. We note that military cyber defence in the EU is at a relatively early stage of maturity, and so these should be understood to be tentative high-level aspects to consider as cyber defence at the EU level evolves. We thus do not assign specific responsibility or a timeframe to take these forward).

Enhancing EU network protection two options might be considered in this regard – either via establishing separate (status quo: European Commission, General Secretariat of the Council (GSC), European External Action Service (EEAS)) or centralised management (Testa, Eurodac, Visa, Operational Wide Area Network (OPSWAN, etc) of data exchange networks

Strengthening intelligence capability – either expansion of the existing efforts with the EU's Situation Centre or creating a new separate co-operative model involving feeds from the European Cybercrime Centre (EC3); ENISA and EEAS.

Deepening incident response capabilities through, for example, separate management (e.g. an EU military CERT) or centralised management (expansion of mandate of existing incident response capabilities e.g. CERT EU or Commission SOCs) and deepen alerts and warnings capabilities for operational HQs.

Creating a culture of cyber-security (good practice, training and awareness raising) by for example either a separate approach or a common approach by extending ENISA's mandate and building upon work done in the EU's Internet Security Task Force which involves other stakeholders (e.g. GSC; EEAS);

Promulgating security standards and tools – either via promoting those already in existence, developing specific of ad-hoc standards or agreeing to deploy NATO standards;

Reinforcing links between NATO and the EU for cyber defence issues including identification of critical infrastructures possibly involved in EU led security and defence missions; NATO-EU exercises involving critical infrastructure operators; establishment within the CERT-EU of a Rapid Reaction Team similar to those within NATO and finally developing a joint cyber-crisis management capability (CERT-EU–NATO Computer Incident Response Capability (NCIRC) or NATO Rapid Reaction Team for the EU under the 'Berlin Plus' agreement).

Recommendations for pMS

Concerning recommendations for the pMS, we offer the following based on the assessment contained in the Maturity Model.

pMS should be encouraged to develop their cyber defence doctrine. This especially in the context of common security and defence policy missions. In addition, pMS can benefit from further guidance with respect to aspects of international strategies for cyber defence.

A watching brief should be kept on how organisational structures evolve to ensure a coordinated response in each pMS. pMS should monitor carefully the development of organisational structures to address cyber defence, noting especially the need to adopt both a policy-level and an operational-level function.

Greater attention should be given to the development of cyber defence training and education initiatives, both at the operational and senior command levels. pMS need to pay attention to the development of cyber defence training, education and skills programmes, not just at the operational level.

pMS could consider exchanging information on equipment solutions and pooling and sharing for cyber defence capabilities, especially in EU-led missions. pMS could exchange information on the deployment of 'best in breed' equipment solutions to cyber defence issues, and consider pooling and sharing certain equipment capabilities.

Exchange of information on practice for the recruitment and retention of cyber defence specialists would be helpful. Here the opportunity exists to exchange best practice on recruitment campaigns and how pMS have addressed the issues of obtaining and retaining the best cyber-security talent.

Processes and shared escalation procedures could be exchanged and developed to execute leadership in cyber defence, especially in the context of EU-led operations. Here we would propose that pMS ought to consider sharing their experience of best practice in devising cyber rules of engagement and escalation mechanisms, in order to address national cyber-security incidents.

pMS could consider to a certain extent sharing facilities and what services are offered within them. pMS could share information on what cyber defence-related facilities are available to contribute to common security and defence policy operations: for example, forensic capabilities, deployable units and so on.

Greater consideration needs to be paid to the interoperability aspects of cyber defence, especially with non-military organisations. pMS would benefit from further guidance on pan-European enterprise interoperability framework models, especially in regard to interactions with non-defence organisations.

Appendix – Background to the Capability Maturity Model

This Appendix describes the capability maturity model, how we developed it, allocated weights to each indicator and what assumptions were used.

Overview

We assign different thresholds which define progress from one level of maturity to the next. These thresholds are different across different capability domains, being based on assumptions stemming from earlier research and our expert judgement. Each capability area is represented by a number of indicators (questions) which have points allocated to them. Progress in each capability area is determined by the minimum number of points required to go from one Maturity level to another. These are in four types, A, B, C and D.

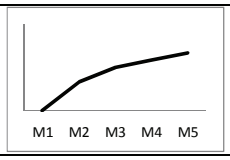
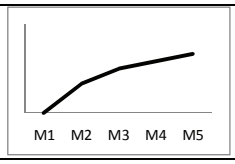
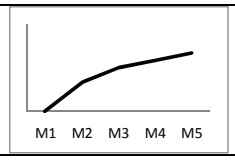
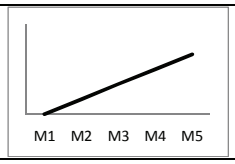
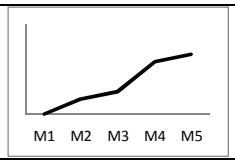
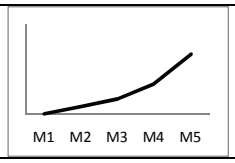
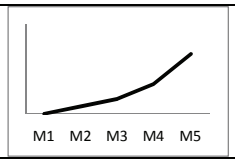
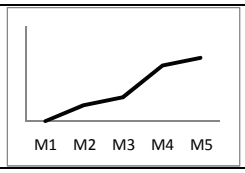
- For some capability domains (specifically "Doctrine" and "Organisation") our model assumes more effort (more points are needed) at the early stages of Maturity (M1 and M2) than later on.[2] This is because in these two capability domains extensive time, resources and effort is required to define and get all relevant stakeholders to agree on a common strategy, or to agree the mandate and role of an organisation.
- For other capability domains namely "Leadership" and "Facilities" our model assumes that less points are needed to progress at the earlier stages (M1 > M2) but then progress becomes difficult (because only then the full enormity of the challenge becomes apparent).
- For the capability domain of Materiel and Logistics (which primarily concerns the deployment of technological solutions) we assume a straight line (linear) progression on the understanding that technology is a neutral tool.
- For the others we assume a more complex 'S' curve which represents a combination of the first two types.

Table A.1 below illustrates this with the number of points required on the vertical axis. It also indicates how we determined the difference in number of points required to transition between each maturity level: ie the 'progression curve' or difficulty level for each capability domain. As can be seen, for different areas there are different difficulty curves depending upon our previous analysis of the complexities of each domain and the assumptions detailed below. For example, for Doctrine, research suggests that this is a capability area which is initially difficult but then once doctrine is more broadly understood, advancing in levels of maturity

[2] A parallel might be made with the gearing on a bicycle. For some 'hills' (military capability areas in our index) there is an easy gradient at the start meaning that progress is initially quite rapid. For other hills is less rapid requiring you to remain in a lower gear and do more work to achieve the same degree of progress.

becomes progressively easier (ie there is an effect of diminishing returns). In other words, all the hard work is done at the start to progress from the early stages of maturity.

Table A.1: Progression curves for maturity level (M*n*) per capability domain.

DOCTRINE	M1	M2	M3	M4	M5	Progression Curve
Percentage Points per M level		50	25	12.5	12.5	
Cumulative percentage points	0	50	75	87.5	100	
ORGANISATION	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage Points per M level	0	50	25	12.5	12.5	
Cumulative percentage points	0	50	75	87.5	100	
TRAINING	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage Points per M level	0	50	25	12.5	12.5	
Cumulative percentage points	0	50	75	87.5	100	
MATERIEL & LOGISTICS	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage Points per M level	0	25	25	25	25	
Cumulative percentage points	0	25	50	75	100	
PERSONNEL	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage points per M level	0	25	12.5	50	12.5	
Cumulative percentage points	0	25	37.5	87.5	100	
LEADERSHIP	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage points per M level	0	12.5	12.5	25	50	
Cumulative percentage points	0	12.5	25	50	100	
FACILITIES	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage points per M level		12.5	12.5	25	50	
Cumulative percentage points	0	12.5	25	50	100	
INTEROPERABILITY	**M1**	**M2**	**M3**	**M4**	**M5**	
Percentage points per M level		25	12.5	50	12.5	
Cumulative percentage points	0	25	37.5	87.5	100	

In summary this means that a particular Maturity level does not necessarily reflect that nothing has been achieved. Depending on the different categories of 'difficulty' per capability domain described above, it might instead be simply indicative of the fact that a lot has been done in a domain where it is *intrinsically* difficult to achieve progress. Conversely, for other capability areas, a higher level of maturity (M5) may require relatively few indicators. These thresholds were also subjected to a sensitivity analysis (+/-10 percent) for the preparation of the country profiles.

Table A.2 below outlines our assumptions about the relative importance of each indicator to each other (within the capability domains).

Table A.2: List of assumptions informing indicators

Capability Domain	Assumptions
Doctrine	We distinguish between *Strategy* – which should informs what objectives should be achieved and *Doctrine* which constitutes a description of how to achieve those objectives. We also make an assumption of a hierarchy of strategies in order of importance (most important at top): 1. A national level cyber-security strategy should be a broad national level instrument outlining what strategy the country needs to take in order to become secure in cyberspace and the objectives, role and mandate (if any) of defence in achieving strategic security objectives 2. A Critical Information Infrastructure Protection strategy is next down the hierarchy, describing the 'what' of the protection of the critical information infrastructure(s) – those technological elements of cyberspace essential for social and economic well-being 3. A cyber defence strategy should describe a desired end-state that the defence and armed forces should work toward achieving to contribute to overall national cyber security objectives across the DOTMPLF-I framework 4. A cyber defence doctrine should outline how this strategy may be achieved through different tools, including CNO but also IA; information sharing; co-ordination with other government departments and the private sector 5. A Computer Network Operations (CNO) doctrine can be thought of as the handbook governing the conduct of various types of CNO • We assume that a national cyber-security strategy and a national CIIP strategy are the two most important building blocks to have in place to move from non-existent level of maturity to initial. • We assume that the presence of a cyber deterrence doctrine and defining cyber attacks as armed attack are indicative of the most mature level. Although they appear as indicators we give them little weight in relation to the others since the background research suggests that they may be ineffectual or even counterproductive.
Organisation	• We assume that the presence of a national level leadership or co-ordinating authority (cabinet office/presidential or prime ministerial level) and an operational level defence organisation are the two equally most important aspects in the organisation domain and both are necessary to progress from a non-existent level of maturity to an initial level of maturity. • We also weight the organisational responsibility for 'defence' being twice as important as for offence, on the basis that cyber offence is generally regarded by experts to be of secondary importance in some cases unnecessary, of far less significance than defence. • The location and function of the unit are contextual and dependent on the specific politico-administrative system in each country (ie how the armed forces are organised). • Given the multidisciplinary, cross cutting nature of cyber defence, we also assume a similar degree of importance respectively to: the inclusion of expertise from other organisations and linkages to national cybercrime capability and/or the national / governmental CERT.

	• Finally, we accord half as much importance to the unit possessing or being linked to expertise from the private sector and other incident response communities (eg product CERTs) as in the context of national security, the national / government CERT would be expected to be the first port of call and interactions with others might only be of lesser benefit.
Training	• We accord an equal weight to cyber security concepts being included in command and staff leadership syllabi and an operational level (as a professional trade or skill within the Armed Forces). This is because, like organisation, it is important both to have training mechanisms in place at the operational level but also a a senior decision-maker level in order to be able to execute effective mission/security trade-offs. • We assume the same level of importance regarding the sharing of good practice and lessons learned on the basis that a lot can also be learned by 'doing' and getting involved in a practical sense. • We assume that participation in EU level exercises and the running of national level recruitment campaigns are half as important as those indicators above. This is because without some policy or strategy to exercise against, such measures are only partially effective • Estimates of theoretical and applied expertise are given weight according to the difficulty curve for this domain. • The indicator regarding the breadth of participants is contextual as being dependent on how extensively the pMS participates in common security and defence policy (CSDP) missions.
Materiel and Logistics	• We assume that for this capability area, there are two overall indicators concerning reliance upon the private sector. Firstly, an estimate of the reliance (1 = not critical and 5 = critical) of the private sector specifically for cyber defence capabilities and secondly estimate of the reliance (1 = not critical and 5 = critical) upon the private sector for ICT in defence more generally. • Each indicator for a specific technology is accorded the same weight in a linear progression of difficulty. Technology is assumed to be neutral and its effectiveness is determined by the other aspects of capability: a state of the art firewall poorly configured may be more detrimental to security than less state of the art technology that is implemented and well managed by highly skilled personnel. • The estimates of total spending in defence on ICT is a nominal figure (as a % of total defence budget).
Personnel	• We accord the most weight to the indicator concerning recruitment and retention of cyber defence specialists as this may be regarded as an important mechanism to attract and retain high quality talent to the military cyber defence capability. • The other indicators are accorded weights in line with the capability domain progression curve for this capability area (as, like technology, they are neutral unless supported by appropriate policies and procedures and highly skilled personnel).
Leadership	• We assume that strategic authorisation for cyber defence capabilities are the most important, then at the operational level and then at the tactical level. This is because of views concerning the possible unintended consequences and the need for clear understanding at a senior level about how to respond to national level incidents. • We also assume that it is important to have a clear escalation mechanism for national cyber security incidents. We assume that having a clear mechanism is as important as having authorisation at the strategic level. • We do not assign a weight to the feasibility of applying a non-national decision to your own networks as this is a preference based on perception. • We assume equal importance to the level of authority (court order; civil

	servant) required to perform surveillance of private sector networks on the basis that this is determined by a complex set of legal and institutional contexts out of the scope of this work.
Facilities	• We assume that different types of facility are more or less important. We assume the most important indicator being the presence of some kind of national level forensics research facility to conduct analysis of malicious code, artefacts of network penetration, Indicators of Compromise (IoC) and so on (although we do not distinguish whether this is in house, provided by another public sector entity – eg law enforcement or even by the private sector). • We assume that a national 'cyber test range' (eg a lab infrastructure where a specific model of parts of cyberspace could be built in order to test capabilities) and a physical facility to address cyber defence (eg a facility to test SCADA vulnerabilities and their impacts on military equipment) is half as important (as they might already be built into the delivery of materiel & logistics by defence contractors) • Finally we assume that the existence of a facility to develop and test offensive capabilities is of least importance out of the four types of facility as developing offensive capabilities is accorded little or low priority by the literature when compared to defensive capabilities • We accord equal weight each to the use of different types of other assets for CD missions as this is a contextual aspect more unique to the particular situation of the pMS, but of strategic importance in the context of EU led CSDP missions.
Interoperability	• The presence of an Enterprise Interoperability Framework (EIF) may be considered as a important indicator in tackling cyber defence as it can support a common understanding of terms (taxonomy), catalogues of available services and interfaces (who should talk to who) between different stakeholders eg operational commanders, ministerial level and service level commands. This is accorded the most weight. • We accord the indicator whether such an EIF is present across other government departments half as much weight • Regarding perceptions as to whether this is sufficiently developed we accord half as much weight again if the respondent indicated that it is sufficiently developed. • Within the level of interoperability, we accord strategic interoperability as the most important, then tactical and then operational. This is because of evidence from the CERT world that shows that tactical (ie technical interoperability) is to a certain extent regarded by practitioners as important

Each assumption is then accorded a weighting or score (number of points) depending upon whether the respondent answers that they do or do not posses that particular indicator. Each score is relative to the others. Not all indicators receive a score. These are detailed in the next section.

Relationship between indicators and maturity levels

Table A.3 below outlines the relationship between indicators in each capability category and the Maturity Index scores. The black cells indicate what we expect to be reported for each maturity level. White cells indicate contextual indicators which are not taken into account at a specific level of maturity. The maturity levels indicate the following: M1 (Non-existent), M2 (Initial), M3 (Defined), M4 (Balanced) and M5 (Optimised).

Table A.3: Relationship between indicators and maturity levels

M1	M2	M3	M4	M5

DOCTRINE						
	Familiarity with CD issues	1	2	3	4	5
	Existence of CS strategy		[redacted]			
	Specific CD strategy			[redacted]		
	National CIIP strategy		[redacted]			
	Computer Network Operations Doctrine			[redacted]		
	Cyber deterrence doctrine					[redacted]
	Cyber-attacks as armed attack?					[redacted]
	Cyber Defence Doctrine				[redacted]	
	International Strategy					[redacted]
ORGANISATION						
	Existence of national steering group		[redacted]			
	Cyber-security org in defence		[redacted]			
	Responsibility for defence & offence?			[redacted]		
	Location of unit					
	Function of unit					
	Expertise from other orgs in unit				[redacted]	
	Expertise from private sector in unit					[redacted]
	linked to national cybercrime capability				[redacted]	
	Co-ordination (linked to n/g CERT)				[redacted]	
	Linked to other incident response					[redacted]
TRAINING						
	CS covered in syllabus at command level?		[redacted]			
	Specific CD training competency/career path or skills profile?		[redacted]			
	Participation in EU exercises					[redacted]
	Estimate of theoretical academic expertise at national level	1	2	3	4	5
	Estimate of applied expertise at national level	1	2	3	4	5
	Conduct national level recruitment competitions?				[redacted]	
	Sharing good practice / Lessons learned			[redacted]		
	Breadth of participants					
MATERIEL & LOGISTICS						
	Reliance upon privately owned assets					
	Perception of role of private sector	1	2	3	4	5
	Perception of role of private sector	1	2	3	4	5
PERSONNEL						
	Recruitment and Retention for CD specialists				[redacted]	
	Identity and Access Management	1	2	3	4	5
	Insider Threat Management	1	2	3	4	5
	Personnel Vetting and assurance	1	2	3	4	5
	Vetting contractors and third parties	1	2	3	4	5
	Recruitment and employment of 'black' or 'grey' hats?	1	2	3	4	5
LEADERSHIP						
	Tactical level of Authorisation for CD capabilities					
	Operational level of authorisation for CD capabilities					

	Strategic level of authorisation for CD capabilities					
	Escalation mechanism for national incidents					
	Feasible to apply a non-national decision to your own network					
	Court order required for surveillance of private sector networks					
	Civil servant authority required for surveillance of private sector networks					
	Other level of authority required for surveillance of private sector networks					
FACILITIES						
	Existence of a national range					
	Dedicated physical facility to address CD					
	Existence of a facility to develop & test offensive capabilities					
	Existence of a national level forensics research facility					
	Use of own assets for CD in CSDP missions					
	Use of NATO assets for CD in CSDP missions					
	Bilateral arrangements with pMS for CD in CSDP missions					
	Bilateral arrangements with non-EU for CD in CSDP missions					
INTEROPERABILITY						
	Sufficient development of CD interoperability					
	Tactical level of interoperability					
	Operational level of interoperability					
	Strategic level of interoperability					

Weighting per indicator

Table A.4 below outlines how we allocated points to each question. For those questions where there was a 1-5 ranking, we allocated points according to the model of progression of each maturity level as per Section B. Many questions noted as contextual where we did not allocate points. For the Material & Logistics Capability area, many countries did not complete these questions so to avoid biases we excluded the analysis of this capability domain from the overall top line results presented at the start of the profile.

Table A.4: Weighting per indicator

Capability domain	Type of question	**Y**	**N**	**D/K**		**Y**	**N**
Doctrine							
Familiarity with CD issues	1-5						
Existence of CS strategy	Y/N	25	-25.0				
Specific CD strategy	Y/N	12.5	0.0				
National CIIP strategy	Y/N	25	-25.0				
Computer Network Operations Doctrine	Y/N	12.5	-12.5				
Cyber deterrence doctrine	Y/N	4.17	0.0				
Cyber-attacks as armed attack?	Y/N	4.17	0.0				
Cyber Defence Doctrine	Y/N	12.5	-12.5				
International Strategy	Y/N	4.17	0.0				
Total max score							*200*
Organisation							
Existence of national steering group	Y/N	25	-25.0				
Cyber-security org in defence	Y/N	25	-25.0				
Responsibility for defence & offence?	Defence or Offence				Defence	25	-25
					Offence	12.5	0
					Other		
Location of unit	Choice (contextual)						
Function of unit	Choice (policy; management of defence only nets; management of defence and civil nets used for defence)				Pol		
					Mgmt Def		
					Mgmt of Def & Priv		
Expertise from other orgs in unit	Y/N	12.5	-12.5				
Expertise from private sector in unit	Y/N	6.25	0.0				
linked to national cybercrime capability	Y/N	12.5	-12.5				
Co-ordination (linked to n/g CERT)	Y/N	12.5	-12.5				
Linked to other incident response	Y/N	6.25	0.0				
Total max score							150
Training							
CS covered in syllabus at command level?	Y/N	25	0.0				
Specific CD training	Y/N	25	0.0				

competency/career path or skills profile?							
Participation in EU exercises	Y/N	12.5	-12.5				
Estimate of theoretical expertise at national level	1-5						
Estimate of applied expertise at national level	1-5						
Conduct national level recruitment competitions?	Y/N	12.5	0.0				
Sharing good practice / Lessons learned	Y/N	25	-25.0				
Breadth of participants	Contextual (choice)				CSDP		
					Bilaterally		
					Non-EU		
					Other		
Total max score							300
Materiel & Logistics							
Reliance upon privately owned assets	Contextual (Y/N)						
Perception of role of private sector	1-5						
(total spending in defence on ICT)	Nominal						
Perception of role of private sector	1-5						
Degree of usage of:							
Perimeter based measures	1-5						
Defence in depth	1-5						
Host based measures	1-5						
PKI	1-5						
Disaster recovery tools	1-5						
DLP	1-5						
Threat intelligence & data fusion	1-5						
Data visualisation	1-5						
Intrusion prevention	1-5						
Honeypots/honeynets	1-5						
Secured messaging / data exchange	1-5						
Forensic platforms	1-5						
Other	contextual						
Total max score							1150
Personnel							
Recruitment and Retention for CD specialists	Y/N	87.5	-25				
Degree of usage of:	1-5						
Identity and Access Management							
Insider Threat Management							
Personnel Vetting and assurance							
Vetting contractors and third parties							
Recruitment and employment of 'black' or 'grey' hats?							
Total max score							637
Leadership							

Level of authorisation for CD capabilities?	Choices (tac; op; strategic)				Tactical	12.5	-12.5
					Operational	25	-12.5
					Strategic	50	-12.5
Clear escalation mechanism for national incidents	Y/N	50	25				
Feasible to apply a non-national decision to your own network	Contextual						
Level of authority required for surveillance of private sector networks	Choices (ct order; civil serv; other)				Court Order	25	-25
					Civil Servant	25	-25
					Other		
Total max score							187.5
Facilities							
Existence of a national range	Y/N	25	0.0				
Dedicated physical facility to address CD	Y/N	25	-12.5				
Existence of a facility to develop & test offensive capabilities	Y/N	12.5	0.0				
Existence of a national level forensics research facility	Y/N	37.5	-12.5				
Use of other assets for CD in the context of CSDP missions	Contextual (choices)				Own Assets	12.5	-12.5
					Those of NATO	12.5	-12.5
					Bilateral arrangements with pMS	12.5	-12.5
					Bilateral arrangements with non-EU	12.5	0
Total max score							150
Interoperability							
Enterprise interoperability framework	Y/N	50	-25				
Common with other government departments	Y/N	25	-12.5				
Sufficient development of CD interoperability	Y/N	12.5	-12.5				
Level of interoperability	Choices (strat; tact; op; other)				Tactical	25	0
					Operational	12.5	0
					Strategic	50	-4.17
					Other (contextual)		
Total max score							175

These weights were also subjected to a sensitivity analysis (+/-10%) above in the preparation of the pMS country profiles.