



DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT



**CYBERSECURITY AND
CYBERPOWER:
CONCEPTS, CONDITIONS
AND CAPABILITIES FOR
COOPERATION FOR
ACTION WITHIN THE EU**

SEDE

EN

2011

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION

DIRECTORATE B

POLICY DEPARTMENT

STUDY

**CYBERSECURITY AND CYBERPOWER:
CONCEPTS, CONDITIONS AND CAPABILITIES FOR
COOPERATION FOR ACTION WITHIN THE EU**

Abstract

The study analyses policy options for strengthening cybersecurity within the EU and examining potential points-of-entry, including within the Common Security and Defence Policy (CSDP). The study provides an overview of the principle concepts and definitions of cyber security and cyber war, drawing attention to the complexity and cross-jurisdictional nature of the field. In addition to examining current cyber threats to the EU, the study also analyses the capacity of the EU to address more sophisticated cyber-attacks within a common framework. In this respect the study offers important insights into the political, operational and structural challenges that need to be addressed in order to protect the EU and its citizens as well and to exercise “cyberpower” on the international stage. The study takes-stock of the existing NATO and EU capabilities related to cyber security and highlights the added value of the EU in applying a diverse range of policies that can help enable it to comprehensively tackle the increasing range of cyber threats. The study has been requested to introduce Members of the European Parliament's Sub-Committee on Security and Defence (SEDE) to the current issues in cyber security and cyber warfare, as well as to provide a selection of policy recommendations, including within the CSDP context. The study also provides innovative conceptual understanding on what might constitute EU “cyberpower”.

This study was requested by the European Parliament's Subcommittee on Security and Defence.

AUTHORS:

Alexander KLIMBURG, fellow/senior adviser, Austrian Institute for International Affairs (OIIIP), AUSTRIA
Heli TIRMAA-KLAAR, research fellow, Estonian Foreign Policy Institute, ESTONIA

Standard briefing carried out within the framework agreement between TEPSA and the European Parliament.

Ref.: EP/EXPO/B/SEDE/FWC/2009-01/Lot6/09

ADMINISTRATOR RESPONSIBLE:

Gerrard, QUILLE
Directorate-General for External Policies of the Union
Policy Department
WIB 06 M 081
rue Wiertz 60
B-1047 Brussels

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Editorial closing date: 15 April 2011.

© European Parliament, [2011]

Printed in [Belgium]

The Information Note is available on the Internet at

<http://www.europarl.europa.eu/activities/committees/studies.do?language=EN>

If you are unable to download the information you require, please request a paper copy by e-mail : poldep-expo@europarl.europa.eu

DISCLAIMER

Any opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation, except for commercial purposes, are authorised, provided the source is acknowledged and provided the publisher is given prior notice and supplied with a copy of the publication.

NOTA BENE: This study had to be re-published due to a formatting error in the table of contents. This error came about during the formatting phase of the document and without the knowledge of the authors.

GLOSSARY

A2TOC	A-GNOSC/ACERT Tactical Operations Centre (US ARMY)
ACERT	Army Computer Emergency Response Teams (US Army)
AFB	Air Force Base
AFIOC	Air Force Information Operation Centre (US)
AFISRA	Air Force Intelligence Surveillance, Reconnaissance Agency (US)
AFIWC	Air Force Information Warfare Centre (US)
A-GNOSC	U.S. Army Global Network Operations and Security Centre
ANG	Air National Guard (US)
APT	Advanced Persistent Threat
ARPANET	Advanced Research Projects Agency Network (US)
ARSTRAT	Army Forces Strategic Command (US)
ASOC	Air and Space Operations Centre (US)
BGP	Border Gateway Protocol
BIX	Budapest Internet Exchange
BMLVS	Bundesministerium für Landesverteidigung und Sport
BND	Bundesnachrichtendienst (GER)
C2	Command and Control (US Army)
C4SIR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (NATO)
CAT	Cyber Action Teams (US)
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CCIPS	Computer Crime & Intellectual Property Section
CCP	Chinese Communist Party
CCTV	Closed Circuit Television
CDR	Commander
CERT	Computer Emergency Response Teams
CHCSS	Chief, Central Security Service (US-NSA)
CI	Critical Infrastructure
CIA	Central Intelligence Agency (US)
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CMC	Central Military Commission (PRC)
CNA	Computer Network Attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COPS	(see PSC)
COREPER	Committee of Permanent Representatives (EU)
COSI	Committee on operational cooperation on internal security
CSC	Council Security Committee (INFOSEC) (EU)
CSIRT	Computer Security Incident Response Teams
CSIS	Centre for Strategic and International Studies
CSS	Central Security Service (US-NSA)
CSSP	Control Systems Security Program

CYBERCOM	US Cyber Command
DARPA	Defence Advanced Research Projects Agency (US)
DC3	Department of Defence Cyber Crime Centre (US)
DDoS	Distributed Denial of Service
DG	Directorate General (EU)
DHS	Department of Homeland Security (US)
DIA	Defence Intelligence Agency (US)
DiB	Defence Industrial Base (US)
DIME	Diplomatic, Information, Military and Economic
DIRDISA	Director, Defence information Systems Agency (US)
DISA	Defence Information Systems Agency (US)
DNS	Domain Name System
DoD	Department of Defence (US)
DodIIS	Department of Defence Intelligence Information Systems (US)
DOJ	Department of Justice (US)
DoS	Denial of Service
EBAO	Effect Based Approach to Operations
EC	European Commission (EC)
EFF	Electronic Frontier Foundation
ELINT	Electromagnetical Intelligence
EU	European Union
EUMC	EU Military Committee
FAPSI	Federal Agency of Government Communications and Information (RF)
FBI	Federal Bureau of Investigation (US)
FEP	Effective Politics Foundation (RF)
FIRST	Forum of Incident Response and Security Teams
FIWC	Fleet Information Warfare Centre
FSB	Federal Security Service of the Russian Federation
FSO	Federal Protective Service (RF)
GAO	General Accountability Office (US Congress)
Gbits/s	Gigabits per second
GBP	Great Britain Pound
GCHQ	Government Communications Headquarters (UK)
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
GRU	Russian military intelligence
GSD	General Staff Department (PRC)
GUO	Russia Main Guard Directorate, predecessor of FSO
GUSTM	Main Directorate for Special Technical Measures (RF)
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IC	Intelligence Community (US)
IC3	Internet Crime Complaints Centre (US)
ICANN	Internet Corporation for Assigned Names and Numbers
IC-IRC	Intelligence Community-Incident Response Centre (US)
ICMP	Internet Control Message Protocol

ICS	Industrial Control System
INC	Integrated National Capability
I-NOSC	Integrated Network and Operations Centre (US)
INSCOM	Intelligence and Security Command (US)
IO	Information Operations
IP	Internet Protocol
ISACs	Information Sharing and Analysis Centres (US)
ISO	Information Security Standard
ISP	Internet Service Provider
IT	Information Technology
IW	Information Warfare
IXP	Internet Exchange Points
JFCC-NW	Joint Function Component Command – Network Warfare
JIOWC	Joint Information Operations Warfare Centre (US)
JP	Joint Publications (US)
JTF-GNO	Joint Task Force Global Network Operations
KSB	Kremlin School of Bloggers
LAN	Local Area Network
LSE	London School of Economics
LSZ Centre	Centre for Licensing, Certification and Protection of State Secrets (RF)
Mbits/s	Megabits per second
MCNOSC	Marine Corps Network Operations and Security Centre (US)
MILDEC	Military Deception
MSS	Ministry of State Security (PRC)
MVD	Ministry of Internal Affairs (RF)
NAC	National Antiterrorism Centre (RF)
NATO	North Atlantic Treaty Organization
NCCT	Network Centric Collaborative Targeting
NCDOC	Navy Cyber Defence Operations Command (US)
NCI-JTF	National Cyber Investigative Joint Task Force (US)
NCO (W)	Network Centred Operations (Warfare)
NCPH	Network Crack Program Hacker
NCRCG	National Cyber Response Coordination Group
NCSC	National Cybersecurity Centre (US)
NCSD	National Cybersecurity Division (US)
NCW	Network Centric Warfare
NMS	National Military Strategy (US)
NNWC	Naval Network Warfare Command (US)
NSA	National Security Agency (US)
NSCC	National Strategy to Secure Cyberspace (US)
NSPD	National Security Presidential Directive
NTOC	NSA/CSS Threat Operations Centre (US)
OECD	Organization for Economic Co-operation and Development
oiiip	Österreichisches Institut für Internationale Politik
OPSEC	Operational security
OSCE	Organization for Security and Cooperation in Europe

OSINT	Open Source Intelligence Investigators
P2P	Peer-to-peer
PSC	Political and Security Committee (EU)
PDD	Presidential Decision Directive (US)
PDoS	Permanent Denial of Service
PLA	People’s Liberation Army (PRC)
PLAF	People’s Liberation Armed Forces (PRC)
PLAN	People’s Liberation Army Navy (PRC)
PRC	People’s Republic of China
PSB	Public Security Bureau (PRC)
PSYOPS	Psychological Operations
RAND	Research And Development - Corporation (US)
RBN	Russian Business Network
RCERT’s	Regional Computer Emergency Response Teams
RF	Russian Federation
RMA	Revolution in Military Affairs (PRC)
RNOSCs	Regional Network Operations and Security Centres (US)
RSSC	Regional SATCOM Support Centres
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signals Intelligence
SITCEN	Situation Centre (EU)
SORM	System for Operative Investigative Activities (RF)
SQL	Structured Query Language
STN	Security Trust Networks
SVR	Foreign Intelligence Service (RF)
TCP/IP	Transmission Control Protocol / Internet Protocol
Telnet	Telecommunication Network
TOC	Tactical Operations Centre
TR-NOCS	Theatre Regional Network Operations Centre (US)
TTP	Tactical Techniques and Procedures (US Army)
UK	United Kingdom
US	United States
USAF	United States Air Force
USD	United States Dollar
USSTRATCOM	United States Strategic Command
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

TABLE OF CONTENTS

GLOSSARY	III
EXECUTIVE SUMMARY	3
1 CONFLICT IN CYBERSPACE	5
1.1 INTRODUCTION: ACTOR CATEGORIES AND THE 'CYBERVEIL'	5
1.2 TYPES OF 'CYBERATTACK'	6
1.3 LEVELS OF 'CYBERATTACK'	7
1.4 KEY CYBER DEFINITIONS	9
1.4.1 Cybercrime	9
1.4.2 Cyberterrorism and Hacktivism	10
1.4.3 'Cyberwar' – A 'Terrible Metaphor'?	11
1.5 INTERNATIONAL LAW AND 'CYBERWAR'	13
2 CYBERPOWER AND CYBERWARFARE CAPABILITIES	14
2.1 'CYBERPOWER' INSTEAD OF CYBERWARFARE?	14
2.2 CHINA – SHORT ANALYSIS	15
2.3 RUSSIA – SHORT ANALYSIS	16
2.4 UNITED STATES – SHORT ANALYSIS	18
2.5 ASSESSMENT	19
3 INTERNATIONAL ASPECTS OF CYBERSECURITY	20
3.1 INTERNET GOVERNANCE AND CYBERSECURITY	20
3.1.1 Technical Internet Governance: ad hoc	20
3.1.2 Policy Internet Governance: institutionalized	21
3.1.3 Informal International Cybersecurity Initiatives	22
3.2 INTERNATIONAL MULTILATERAL ORGANIZATIONS AND CYBERSECURITY	23
3.3 UNITED NATIONS AND CYBERSECURITY	25
3.4 NATO CYBERDEFENCE INITIATIVES	26
3.5 ASSESSMENT	27
4 CYBERSECURITY IN THE EUROPEAN UNION	29
4.1 THE NATURE OF EUROPEAN CYBERSECURITY	29
4.2 CYBERATTACKS, CYBERCRIME AND CYBERTERRORISM	29
4.2.1 Key Documents and Strategies	29
4.2.2 Key Programs and Institutions	31

4.3	NETWORK AND INFORMATION SECURITY, CIIP AND CIP	31
4.3.1	Key Documents and Strategies	32
4.3.2	Key Programs and Institutions	33
4.4	COMMON FOREIGN AND SECURITY POLICY MEASURES	34
4.5	ASSESSMENT: EU INITIATIVES	35
4.6	KEY CYBERSECURITY ORGANIZATIONS IN SELECTED EU MEMBER STATES.	36
4.6.1	Large Advanced Member States	37
4.6.2	Medium and Small Advanced Member States	38
4.6.3	Other Member States	39
4.6.4	Overall Member States Assessment	40
5	ASSESSMENT AND RECOMMENDATIONS – 23 POINTS	41
5.1	ASSESSMENT	41
5.2	RECOMMENDATIONS	44
5.3	CONCLUDING	47
	APPENDIX I: TYPES OF CYBERATTACKS – A PRIMER	48
	APPENDIX II: LEVELS OF CYBERATTACKS – EXAMPLES	51
	APPENDIX III: LIST OF MOST SIGNIFICANT CYBERATTACKS 2010	54
	APPENDIX IV: CHINA: MILITARY, NETIZENS AND PATRIOT HACKERS	55
	APPENDIX V: RUSSIA: SILOVIKI, CYBERCRIME AND HACKER PATRIOTS	58
	APPENDIX VI: THE US: CYBEROPS, PRIVATE BUSINESS, AND ‘WHITE HATS’	61
	APPENDIX VII: EU M.A.D.R.I.D. REPORT TIMETABLE FOR CYBER	65
	BIBLIOGRAPHY	66

EXECUTIVE SUMMARY

We are in the midst of a cyber war of words
--Howard Schmidt at the 2011 RSA conference¹

As can be expected from the advent of a new medium, the debate regarding cybersecurity and cyberwarfare is intricate, complex, and beset with ambiguities and seeming contradictions. Even the spelling of the very terms themselves is still a matter of debate. In such an environment there are few terms that remain uncontentious.

'Cyberwar' is one of these contentious terms. It has been called a 'terrible metaphor', and has often been used in widely inappropriate settings. At its most useful definition, cyberwar implies that interstate conflict can have a special dimension in the cyberspace domain, and that this domain is quite unlike other military domain of conflict, such as air or sea. In a wider interpretation, 'cyberwar' is also symptomatic for a new type of conflict, one in which interstate aggression is effectively constant, the battlefield is informational and the spoils are knowledge and behavioural change.

Definitions matter, and the term 'war' should certainly never be used lightly in international politics. What is certain is that any discussion of cyberwarfare cannot be had without discussing cybersecurity. Cybersecurity encompasses the defence against all types of cyberattacks, and includes a number of related issues not normally associated with cyberwarfare or even foreign policy, including critical infrastructure protection, Internet governance, cybercrime, data protection, and others. Indeed, the current debate among experts tries to merge these different components into cohesive policy structures that can be applied to international affairs - an integrated concept of 'cyberpower', rather than independent discussions on cyberwarfare and cybersecurity.²

The present study, conducted at the request of the European Parliament AFET/SEDE,³ examines the specific issues of 'cyberwarfare and cybersecurity' pertaining to the EU Common Foreign and Security Policy (CFSP) and provides both an assessment as well as recommendations for further action. The study shows that CFSP-relevant cybersecurity extends further than simply understanding military cyberattacks and includes a wide range of themes, from critical infrastructure protection in EU Member States to global discussions on Internet governance, that need to be holistically connected.⁴

Part 1 of the study **provides an overview of conflict in cyberspace**. Most importantly, it emphasises the need to understand ambiguity when discussing cybersecurity. The cyberactors, the activities they engage in, and even the types of cyberattack they execute are often not easily classifiable. Worse, such a classification can even be misleading – a criminal actor can also be a governmental/military actor, and indeed vice versa. Ambiguity is a reality in cyberspace.

¹ Quoted from Doyle, Eric, 'RSA: Cyber War Mass Hysteria Is Hindering Security', eWeekEurope, 17 February 2011, <http://www.eweekeuropa.co.uk/news/rsa-cyber-war-mass-hysteria-is-hindering-security-21276>.

² The authors prefer to use the term 'cyberpower' to cover the whole range of issues involved in interstate cyber-conflict, rather than 'cyberwar'. The term 'cyberwar', when used, refers to the military application of cyber-means, or the application of state cyber-capabilities for 'war-like' purposes. The term 'serious cyberattack', when used, refers to any type of cyberattack waged by both state or non-state actors that has serious consequences for national security, internal security, economic security, or public safety.

³ Committee on Foreign Affairs (AFET), Subcommittee on Security and Defence (SEDE)

⁴ Within the constraints of this study it is not possible to provide a comprehensive analyses, but appendixes have been added to help with further understanding

- Part 2 **explains the concept of cyberpower**, and gives very brief analyses of the world's largest cyberpowers – Russia, China and the United States. Special attention is paid to the importance of the non-state actors in each case, and how different countries can seek to coerce, co-opt or simply convince their non-state actors into cooperation with the state.
- Part 3 **introduces the different aspects of international cybersecurity**. With the growing importance of the Internet, governments have shown an increasing interest in Internet governance. International organizations as well as nation-states have become increasingly involved in a field formerly dominated by non-state actors. The UN has a dual role, both as an increasingly relevant forum for nation-states to discuss international law and cyberwarfare, but also as an institutional actor within Internet governance. A section on NATO illustrates how challenging it can be for an international organization to make progress on cybersecurity.
- Part 4 **summarizes the major EU policy initiatives on cybersecurity**. Activities concentrating on fighting cybercrime and increasing Network and Information Security (NIS) have provided important support to the development of European 'resilience' to serious cyberattack. However, a near total lack of CFSP engagement in this topic – as well as weak coordination among the EU institutions themselves – have meant that the ability of the EU to measurably project 'cyberpower', or even deal with serious cyberattacks, is very limited indeed. A short survey of some Member State's capabilities shows the large differences in cybersecurity preparedness within the Union, and the important role the EU can play in assisting the development of national capabilities.
- Part 5 **provides 23 assessments and recommendations** on the state of EU cybersecurity, which elements will constitute EU cyberpower, and offers ideas on steps that should be taken to address the most critical current shortfalls. Important issues include the need for urgent improvement of the EU institutions' own cybersecurity measures and streamlining the institutional responsibilities, as well as the increase of resources to develop capabilities both within the EU institutions and the Union as a whole. The EU would benefit from better coordination of the existing initiatives and programs, and a new 'CFSP cyber agenda' could help connect the CFSP with well-established EU cybersecurity initiatives as well as assisting to determine the response mechanisms to serious cyberattacks.

The contribution of the European Union to the overall cybersecurity of Europe has been mixed. The EU has played a very important role in helping to develop EU-wide resilience measures against cyberattacks. However, there are significant differences between the individual Member State cybersecurity capabilities, and the EU institutions themselves are poorly protected. Furthermore, there is currently little CFSP engagement in the EU Cybersecurity debate, despite the obvious relevance of the subject to European peace and security. Without proper political attention, higher-level awareness and Union-wide frameworks to manage cybersecurity both internally and internationally, the ability of the EU to 'project cyberpower', or even the ability to prevent or manage serious cyberattacks, remains limited.

1 CONFLICT IN CYBERSPACE

Cyberspace means the interdependent network of IT infrastructures, and includes the Internet, telecoms networks, computer systems, and embedded processors and controllers in critical industries

—NSPD 54 2008⁵

Cyberspace. A consensual hallucination

—William Gibson, 1984⁶

'Cyber' as a prefix is as old as the first computers.⁷ Despite this ancient pedigree, the confusion over how to apply the prefix cyber has not decreased recently – far from it: terms like cybercrime, cyberterrorism and cyberwarfare are increasingly used, although often with unclear definitions. Mostly, the context is one particular rising threat – the threat of criminal networks, or of international terrorism, or of an aggressive nation-state's foreign policy. The tendency is to view these threats in isolation from each other, and to view the technical commonality of computer and computer networks as the single encompassing factor – i.e. 'cyber'. In reality, the difference between these threats is often razor thin, or solely in the eye of the beholder. Most cyberthreats involve elements of loosely connected networks and actors with rapidly shifting identities, whereas government responses tend to take place within pre-existing institutional settings. Cyber-identities tend to be highly amorphous and ambiguous, but most governments have difficulty dealing with ambiguity. When discussing any type of conflict in cyberspace, it is therefore necessary to understand the fluidity of actor-categorisations, and what these actors may, and may not, have in common.

1.1 Introduction: Actor Categories and the 'Cyberveil'

The differences between cybercrime, cyberterrorism and cyberwarfare are often difficult to ascertain, and often lie in the eye of the beholder. The reasons for this are not only technical, although the physical reality of the Internet means that identifying an attacker is no easy matter. Rather, a principle problem with the separation of cyberattacks into such actor-based categories as 'criminal', 'terrorist' and 'soldier' is that in fact these identities themselves can be fluid and ambiguous. Even if the attacking individual can be identified, it is perfectly possible for a cybercriminal to engage in cyberwarfare acts disguised as a cyberterrorist. Likewise, what is actually cybercrime can sometimes be misunderstood as an act of cyberwarfare – or a cyberterrorist might try to impersonate a state 'cyberwarrior', with potentially serious consequences. Ambiguity is a state of reality in cyberspace.

The problem of assigning such clearly distinct actor categories and the policy recommendations associated with them has been an obvious challenge for a number of years. Most Western nations have found it difficult to appreciate the ambiguity of cyber-actors and indeed cyberattacks, preferring to classify according to traditional government structures such as 'internal security', 'police', or 'military'. As

⁵ National Security Presidential Directive/NSDP 54, Cyber Security and Monitoring, p. 8.

⁶ Gibson, William, *Neuromancer*, New York, Ace Books, 1984, p. 67.

⁷ *Cyber*, from the Greek for 'skill of nautical navigators', was first applied to data-systems as far back as 1948 (see, for example, Wiener, Norbert, *Cybernetics or Control and communication in the animal and the machine*, New York, John Wiley, 1948.).

observers in China and Russia have realized for years, this bureaucratic breakdown is not useful at all. An article in a Russian military journal from 2007 declared that

"isolating cyberterrorism and cybercrime from the general context of international information security is, in a sense, artificial and unsupported ... it is primarily motivation that distinguishes acts of cyberterrorism, cybercrime, and military cyberattacks ... [without knowing the motivation one cannot] qualify what is going on as a criminal, terrorist or military-political act. The more so that sources of cyberattacks can be easily given a legend as criminal or terrorist actions."⁸

This reflects what has long been presumed to be a basic assumption of cyberpower in Russia, China and perhaps elsewhere: non-state actors can be used by the state, overtly or covertly, to execute plausibly deniable cyberattacks.

A defining reality of cyberattacks is that even with the most advanced intelligence-collecting abilities, it is unlikely that a proficient cyberattacker can be definitively identified.⁹ In the Internet, individual data packets do not come with a unique identifier – real-time attribution can be extremely difficult, and even post-attack forensic attribution can deliver uncertain results. Some forms of attack are easier to attribute than others, in particular Computer-Network Exploitation (CNE, usually computer espionage and the theft of sensitive data, see below). As data has to be 'exfiltrated' (that is, it has to travel back to the attacker), such attacks are more readily traceable. This means, however, that states have an interest in maintaining or tolerating political or criminal organizations that, if necessary, can take part in state-sponsored cyberattacks. There is ample evidence to suggest that many states do exactly that, and utilize these non-state groups in cyberattacks against other nations.

As actor attribution is a serious challenge in cyberspace, there are many observers who advocate abandoning efforts at all such actor-based or motivation-based attribution, and instead to concentrate on overall 'cyberdefence', on providing cybersecurity against all kinds of cyberattacks. Operationally this makes little sense¹⁰ – having, as used by the United States until 2010, a national cyber-incident management mechanisms based on actor-attribution (i.e. crime, terrorist, or war) is very likely a recipe for considerable confusion in case of a major cyberattack. Strategically and politically, however, having actor/motivation categorisations does make sense, as they do address different legal and policy considerations that are bedrock issues of international security, and are unlikely to change greatly in the next decade. Talking of cybercrime, cyberterrorism and cyberwarfare does, therefore, make sense – if only to understand better what cyberwar is not, rather than what it is.

1.2 Types of 'Cyberattack'¹¹

Cyberattacks can include a wide-range of technical and social methods to pursue an ultimate goal – the propagation, extraction, denial, or manipulation of information. The US military, in particular, has

⁸ Russian Federation Military Policy in the Area of International Information Security, 'Regional Aspect', *Military Thought*, vol. 16(1), January 2007.

⁹ There have been repeated indications that the US intelligence community in particular has developed special methods of actor attribution. Ian Lobban, head of the UK's GCHQ, speaking at the IISS on 12 October 2010, followed US Deputy Secretary of Defence William J. Lynn in hinting attribution was sometimes possible, 'but it was very, very hard' (Lobban, Ian, 'Speech at the IISS', GCHQ, http://www.gchq.gov.uk/press/cyber_iiiss.html).

¹⁰ The authors of this study will also often use the term 'serious cyberattack' when referring to operational measures, as it will often be uncertain at the time if an attack is e.g. a terrorist act or effectively one of war. Many of the protection and response mechanisms would remain the same in any case.

¹¹ An overview of these attack methods (incl. 'hacking', 'DDoS'; 'trojans' etc.) is included in Appendix I of this study. It is suggested that non-experts read Appendix I for background information.

engaged in an extensive analysis of cyberattacks, and its definitions are widely used today – even though these definitions are generally considered to have weaknesses. The terminology used is not always completely appropriate for all activities, especially those of ‘cybercrime’, but it does cover the majority of attacks and attack-types experienced in cyberspace.

The military definition of cyberattacks is largely covered with the term ‘Computer Network Operations’ (CNO). CNO itself includes ‘Computer Network Attack’ (CNA), ‘Computer Network Exploitation’ (CNE), and ‘Computer Network Defence’ (CND). CND includes a wide number of different approaches and organizations, the most significant of which are specific bodies often known as CERTs (Computer Emergency Response Teams), and which also represent a basic element of civilian cybersecurity. CNA is defined as ‘Operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves’,¹² while CNE is defined as ‘enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.’¹³ These definitions therefore effectively differentiate ‘offensive actions’ (CNA) and ‘espionage’ (CNE) – the former being most likely an act of war, the latter most likely not.

This segmentation has been problematic for a number of reasons, not the least because, technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyberwarfare can well be cyberespionage initially – or simply be disguised as such.

1.3 Levels of ‘Cyberattack’¹⁴

A US military model¹⁵ in use since 2008 has increasingly been used to break down cyberattacks into groups according to the level of sophistication and impact. Although, in the opinion of the authors, this model has significant limitations, it is closest to a ‘standard’ breakdown of cyberattacks and is often used by the US Department of Defence.¹⁶

According to the so-called AF-SAB model, there are three levels of (military-relevant) cyberattacks¹⁷

- **Level 1** has been called ‘**network wars**’, or also ‘system administrator versus system administrator.’ Mobile malicious logic, Trojan attacks, basic phishing attempts, common exploits, website defacement and other ‘common headaches’ fall within this category. Other US government observers have defined this as the ‘CNE’ level, implying that ‘cyberespionage’ can have a cyberwar dimension. Level-1 cyberattacks represent the vast bulk of all cybercrime activity, as well as most of the purported state-sponsored cyberespionage attacks on governments, such as the ‘Moonlight Maze’ and ‘Titan Rain’ campaigns¹⁸. The implication is that these attacks, despite their real-work consequences, are still among the least serious of all attacks, and can largely be addressed through ‘proper network security precautions’.

¹² Joint Publication (JP) 3-13, *Information Operations*, 2006, http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

¹³ Ibid.

¹⁴ A considerably more detailed explanation of the different levels of cyberattack, including historic examples, has been provided in Appendix II.

¹⁵ The AF-SAB model refers explicitly to ‘cyberwarfare’, however an interpretation of this is that the model refers to ‘military cyberattacks’ rather than seeking to impose a legal theory on what constitutes a state of war in cyberspace.

¹⁶ See Garamone, Jim, ‘Lynn: NATO must get ahead of Cyber Threat’, *American Forces Press Service*, 25 January 2011, <http://www.defence.gov/news/newsarticle.aspx?id=62572>.

¹⁷ Quoted from Mudge, Raphael S. and Lingley, Scott, ‘Cyber And Air Joint Effects Demonstration (CAAJED)’, Air Force Research Laboratory Information Directorate, March 2008, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA481288>.

¹⁸ See Appendix II.

- **Level 2** is labeled as **‘cyber-adjunct to kinetic combat’**. A level 2 attack is one where an operator tries to achieve a ‘kinetic effect’ through a cyberattack, i.e. the denial or disruption of an IT-based system, usually in conjunction to an conventional attack, such as an air-strike. The use of malicious logic to disable an air-defence network is an example of a level 2 attack. Other observers have more pointedly (and perhaps incorrectly) referred to this as the ‘DdoS’¹⁹ level – implying that some types of Denial of Service attacks (depending how equivalent to a ‘kinetic attack’) can be compared to a medium-level cyberwarfare attack. As always, outcomes are decisive in deciding to which group the attack can be assigned. This does not mean that the 2007 Estonia attacks would have constituted a cyberwarfare attack, but that Georgia 2008 may have (due to the ‘real-life’ implications of having communications disrupted during kinetic combat).
- **Level 3**, the most dangerous, is **‘malicious manipulation’**. The AF-SAB report claims these attacks are ‘the ones to be feared, they are covert, they are planned, they are orchestrated, and they can cause widespread havoc and disruption without the victims realizing their problems are cyber related.’²⁰ Effectively, these attacks refer to both wide-scale manipulations of systems with evident and immediate effect (for instance a gas pipeline or power generator, with explosive results) or covert manipulation which goes unnoticed over time (for instance with Stuxnet). Depending on systems under attack and the exact intent, these operations are usually beyond the means of non-state actors. However, non-state actors can certainly support such operations – for example different cybercrime actors being hired to program and support such an attack.²¹

The AF-SAB model described above is not universally accepted, even by the US military. There is a clear emphasis on military-tactical ‘battlefield cyber-missions’ (such as supporting an air strike) rather than military-strategic or political missions. The application of the military escalation formula ‘disrupt’, ‘deny’ and ‘destroy’ is potentially too linear. There are a number of specific issues as well. The relatively low ranking of Level-1 attacks masks the fact that literally hundreds of billions of Euros’ damage is caused to OECD economies by cyberspionage, be it criminal or state origin. Also, the national security implications of having a wide range of government systems regularly penetrated and their information revealed is hardly a minor nuisance. Level 2 attacks, despite their potential ‘kinetic effect’, do not necessarily cause more damage or present a greater risk than Level 1 attacks – arguably the opposite is true. Level 3 attacks also conceal a wide range of possible behaviour – this can include the simple manipulation of a spreadsheet, to Stuxnet and similar purported limited attacks on critical infrastructure, to mass-casualty attacks on an entire nation’s critical infrastructure or even the misrouting of the Internet itself.²²

Despite these limitations, the AF-SAB model (interpreted for ‘cyberattack’ and not for ‘cyberwarfare’) is to a certain extent useful, especially as it blends both sophistication of attack and outcome. The interesting implication of this model is that ‘intent’ is of relatively secondary importance – if the overall intent of the attacker is to cause mass mayhem, but the skills employed are very basic and can be defeated through proper network security behaviour, then a potential Level 3 attack would never become more than Level 1. This puts the onus on the defender to ‘do the job right’, rather than the

¹⁹ ‘Distributed Denial of Service’ refers to an attack where an individual computer is flooded with information from many other computers, forcing it to slow, shut-down or malfunction. The attacks are conducted via ‘botnets’ of hijacked computers (see: Appendix I and II).

²⁰ Mudge and Lingley, 2008, p. 1.

²¹ See Appendix I and II.

²² A number of cases were reported in 2009-10 where a (usually Chinese) name server temporarily ‘contaminated’ the Internet Domain Name System (DNS) at a Root level. This theoretically meant that a large section of the world-wide Internet traffic could have been briefly routed through China (see Appendix I).

attacker to constrain his actions. As former CIA director General Michael Hayden recently said: 'If you try to steal my information, and I let you – then shame on me.'²³

1.4 Key Cyber Definitions

1.4.1 Cybercrime

Cybercrime is one of the most pressing security concerns in today's networked world. This is not only because of the sheer scale of cybercrime, but also because the ambiguous nature of actors in cyberspace means that cybercriminals can really be (state-backed) cyberwarriors – and vice versa. Many of the attack techniques used are largely the same. Addressing and combating cybercrime therefore address many of the operational issues potentially associated with cyberwarfare; thus it has become a focus for national security policies in many countries.

Cybercrime is increasingly considered to be the most advanced and profitable of all criminal enterprises – estimates of the cost of cybercrime to business range as high as 1 trillion dollars for 2009,²⁴ and it has long since overtaken the drug trade in terms of business volume.²⁵ The structure and nature of cybercrime is highly diverse and difficult to isolate – in the last couple of years, however, some aspects of cybercrime have become increasingly relevant to international security policy. The ability of sophisticated 'cyber-gangs' to leverage entire logistic networks makes them a factor directly relevant to government cybersecurity efforts, and even to cyberwarfare and cyberterrorism. A major cybercrime syndicate, the Russian Business Network (RBN), was even identified by NATO as being a direct threat.²⁶ In the United Kingdom, cybercrime was recently identified as one of the four most serious threats to national security.²⁷ Cybercrime activities can include a wide swath of activities that impact both the individual citizen directly (for instance, identity theft) and corporations (for instance, the theft of intellectual property). At least as significant for national security, however, is the logistical support capability cybercrime can offer to anyone interested in conducting cyberattacks. This includes hosting services, the sale of stolen identities and credit card numbers, money-laundering services,²⁸ and even the provision of entire hacking tools and root-kits to enable large-scale cyber-campaigns.²⁹ There are strong indications that Russian cybercrime syndicates played a role in the cyberattacks on Georgia and Estonia,³⁰ to name but two examples. Stuxnet, a cyberweapon purportedly launched at the Iranian

²³ Comments made by Hayden, Michael, *Comments at the Georgetown University Conference on International Engagement in Cyberspace*, 29 March 2011, <http://lsgs.georgetown.edu/programs/CyberProject/InternationalEngagement/>.

²⁴ See Mills, Elinor, 'Study: Cybercrime Cost Firms \$1 Trillion Globally', *cnet news*, 28 January 2009, http://news.cnet.com/8301-1009_3-10152246-83.html.

²⁵ See Leyden, John, 'Cybercrime 'More Lucrative' than Drugs. At least phishing fraudsters don't have Uzis', *The Register*, 29 November 2005, <http://www.theregister.co.uk/2005/11/29/cybercrime/>.

²⁶ See Newsweek, *The (Evil) Cyber Empire. Inside the world of Russian hackers*, 30 December 2009, <http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html>.

²⁷ See, for example, UK Government, *A Strong Britain in an Age of Uncertainty. The National Security Strategy (UK-NSS)*, October 2010,

http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.

Specifically, the UK-NSS refers to 'cyberattack' as the threat, which said to encompass cyberespionage by both criminal and state organizations.

²⁸ See Kirk, Jeremy, '5 Indicted in Long-running Cybercrime Operation', *csoonline*, 2 September 2009, http://www.csoonline.com/article/501180/5_Indicted_in_Long_running_Cybercrime_Operation.

²⁹ For an early mention of this see BBC, *Cyber crime tool kits go on sale*, 4 September 2009, <http://news.bbc.co.uk/2/hi/technology/6976308.stm>.

³⁰ See Project Grey Goose, *Phase I Report: Russia/Georgia Cyber War – Findings and Analysis*, 17 October 2008, <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>; Idem, *Phase II Report: The evolving state of cyber warfare*, 20 March 2009, <http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>; and US Cyber

nuclear program by Israel and/or the United States, may have been written with the help of cybercriminals.³¹ Finally, there is significant evidence that implicates non-state groups (possibly definable as cybercrime groups) in serious cyberespionage cases directed against Western governments. Due to the difficulty of actor attribution, as well as legal consequences in categorizing an attack as 'warfare', it can be presumed that many of the anti-cybercrime security measures European governments seek to implement are at least equally directed at state-directed cyberattacks.

1.4.2 Cyberterrorism and Hacktivism

The concept of 'cyberterrorism' is highly contentious. The term has been used in a wide range of contexts, many of them disputed, and most of them used only in the US. The FBI has reportedly defined cyberterrorism in terms very similar to their conventional terrorism definition.³² The US Army developed two definitions of cyberterrorism, namely 'activities carried out in support of conventional terrorism' (e.g. 'content', such as propaganda, recruitment, or planning) and actual 'cyberattacks for terrorist purposes'. The 'content' interpretation of cyberterrorism raises many obvious concerns, as it can quickly cross over into civil-rights and freedom of expression issues. The category 'direct cyberterrorist attacks' is not undisputed either, as this also includes a wide range of behaviour, not all of which can be considered as serious-attacks. There have certainly been a number of politically-motivated non-state attacks on the Internet, ranging from website defacement operations to attacks on entire countries. In Europe, the so-called 'cartoon controversy' led to a number of effective 'online Jihadi' cyberattacks against Dutch, Swedish and especially Danish websites between 2006 and 2008.³³ In 2007, Estonia suffered a wide-ranging politically-motivated cyberattack that it also referred to as a cyberterrorist attack.³⁴ The production of computer viruses for ideological reasons or for purely disruptive, non-financial gain could be termed a cyberterror attack.

Overall, a strong concern exists that applying the term cyberterrorism loosely (or in any form at all) would allow draconian security legislation to be applied to relatively minor misdemeanours. A number of critics have therefore sought to completely replace the term cyberterrorism with terms such as 'hacktivism' or 'cyber-mob'. Sometimes it is argued that attacking a website, or a network, can never be considered terrorism, as direct casualties hardly ever result – in other words, if there are no direct casualties it cannot be considered terrorism. This argument ignores, however, the fact that mass disruptions on their own can be extraordinarily expensive to a society or an organization, potentially crippling a country's economy or destroying a company. The widely accepted difference between 'terrorism' and 'vandalism' and 'hacktivism' (or similar nuisance-level attacks) is the actual amount of damage caused. Large-scale disruption of public services, even in the absence of direct casualties, has often been considered an act of terrorism.³⁵ 'Nuisance' or 'inconvenience' attacks are generally not considered terrorist activities.

Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign Against Georgia in August 2008*, August 2009, <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

³¹ See Farwell, James P. and Rohozinski, Rafal, 'Stuxnet and the Future of Cyber War', *Survival*, vol. 53(1), 2011, pp. 23-40.

³² US Army TRADOC, *Cyber Operations and Cyber Terrorism*, 15 August 2005, <http://www.scribd.com/doc/2514092/Army-TRADOC-G2-Handbook-No-1-02-Cyber-Operations-and-Cyber-Terrorism>.

³³ See Stohl, Michael, 'Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?', *Crime, Law and Social Change*, 46(4-5), 2007, pp. 223-38.

³⁴ See Bloomfield, Adrian, 'Estonia calls for NATO cyber terrorism strategy', *The Telegraph*, 18 May 2007, <http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html>.

³⁵ One European example of this was the Southern Tyrol Liberation Committee attacks on a number of Italian electricity pylons, which led to wide-scale disruptions of services (see Schmid, Alex P. and Jongman, Albert J., *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, & literature*, New Brunswick and New Jersey, Transaction Publishers, 2005.).

It needs to be pointed out that 'cyberterrorism' as a label can even have a potentially de-escalatory effect in international relations. In cases where a serious cyberattack³⁶ is only attributable to a general country, rather than an organization in a country, the concept can help avoid inadvertent escalation between nation-states.

1.4.3 'Cyberwar' – A 'Terrible Metaphor'?

'Cyberwar,' noted expert James Lewis once said, 'is a loaded term'.³⁷ There is no common definition of what might constitute 'cyberwarfare'. The 2007 attacks on Estonia, the 2008 attacks on Georgia, the deployment of Stuxnet, or the on-going high level of cyberespionage were all called cyberwar at one point. Even cyberattacks that most likely have nothing to do with conflicts between states, such as the 'hactivist' cyberattacks in the wake of the 2010 Wikileaks affair or in support of the February-March 2011 Arab revolts have been titled as cyberwar, implying, in effect, that the category of warfare is not limited anymore to mere nation-states. In the absence of a common definition, most EU Member States and the Commission have studiously avoided using the term cyberwarfare in official documents, and often prefer neutral terms such as 'cyberespionage', 'cyberattack'³⁸ or 'cyberdefence'. These are not attempts to deny the existence of state-directed cyberattacks, or the potential of cyberweapons to wreak havoc, but rather based on the awareness that 'war' is, among other things, a legal term whose use by government should certainly not be taken lightly. While the term 'cyberwar' has little meaning legally, it can be argued that cyberwar is meaningful as a conceptual tool to express different levels of interstate conflict through and within cyberspace. That such a conflict can and does exist, and can encompass various levels of behaviour, is not in dispute.

The Internet security company McAfee has warned since 2007 that, in its opinion, a 'virtual arms race' is occurring in cyberspace – with a number of countries deploying cyberweapons.³⁹ Many governments are building capabilities to wage cyberwar,⁴⁰ while some NATO reports have claimed that up to 120 countries are developing a military cyber-capability.⁴¹ These capabilities can be interpreted as simply one more tool of warfare, similar to airpower, which would be used only within a clearly defined tactical military mission – for instance for shutting down an air-defence system. This can be described as 'operational cyberwarfare' or 'cyber as an enabler', and reflects more the integration of cyberattacks into future conflict scenarios than anything else,⁴² and is mostly equivalent to the Level-2 cyberattacks in the AF-SAB model (above). Alternatively, the emphasis can lie on 'strategic cyberwarfare' – the ability to strike at the heart of an (advanced) nation by undermining its economy and its basic ability to function. These attacks can also be described as Level-3 cyberattacks according to the AF-SAB model. Unlike other forms of conflict, 'strategic cyberwarfare' can be waged only within the cyberspace domain, can achieve wide-scale disruption without destruction, and can even be waged without the perpetrator being positively identified. While traditionally the West has primarily focused on the first interpretation

³⁶ See Bloomfield, 2007.

³⁷ See Jackson, William, 'How can we be at cyberwar if we don't know what it is?', *Washington Technology*, 22 March 2010, <http://washingtontechnology.com/articles/2010/03/22/cybereye-cyberwar-debate.aspx>.

³⁸ See, for example, UK Government, 2011.

³⁹ See Zeenews, *US, China, Russia have 'Cyber weapons': McAfee*, 18 November 2009, <http://www.zeenews.com/news579965.html>.

⁴⁰ See, Cheek, Michael W., 'What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare'', *The new new Internet – The Cyber Frontier*, 2 March 2010, <http://www.thenewnewinternet.com/2010/03/02/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>.

⁴¹ See Hale, Julian, 'NATO Official: Cyber Attack Systems Proliferating', *DefenceNews*, 23 March 2010, <http://www.defencenews.com/story.php?i=4550692>.

⁴² An example of how all future conflict can be viewed as being increasingly influenced by cyber-technology is the new term 'Cybered Conflict' (see Demchak, Chris, 'Cybered Conflict vs. Cyber War', *Atlantic Council*, 20 October 2010, http://www.acus.org/new_atlanticist/cybered-conflict-vs-cyber-war).

(‘cyber as an enabler of conventional operations ’), the concept of ‘strategic cyberwar’⁴³ has increasingly gained acceptance in policy debates.

Exactly how susceptible an industrialized country would be to such a serious cyberattack has been subject of a wide-ranging debate. The most recent of the so-called ‘Electronic Pearl Harbor’ scenarios was presented in a 2010 publication by a US government insider.⁴⁴ It raised the specter of a devastating cyberattack leading to the wide-scale collapse of the US infrastructure, with massive casualties and a ruined economy, without it even being clear who the attacker was. Despite the book having been dismissed out of hand in a recent OECD-study,⁴⁵ it is increasingly accepted in policy circles that severe and debilitating attacks on heavily industrialized nations can indeed be waged by cyber-means, even if only with a considerable investment in resources and the utilization of a wide range of different approaches.⁴⁶ Such resources can most likely only be fielded by a state-actor, although a recent US cybersecurity exercise illustrated that such an attack could plausibly be executed by a non-state actor as well.

In recent years most of the (US-dominated) debate on cyberwar has either been orientated towards ‘Resilience’⁴⁷ or ‘Deterrence’.⁴⁸ Recently the Obama administration⁴⁹ has seemed to increase its support of ‘Resilience’- based approaches to overall cybersecurity and cyberwarfare.⁵⁰ The US cybersecurity ‘czar’, Howard Schmidt, speaks for many in the field when he derides cyberwarfare as a ‘terrible metaphor’⁵¹ for attacks such as cyberespionage, stating that this language ‘distracts from the real job of making the networks more secure.’⁵² Cyberdeterrence is instead mostly marked by a proven ability to impose unacceptable costs on a potential attacker through various forms of retaliation.⁵³ A central contention here, often voiced by the military community, is that the attacker will be apparent, based on other factors (such as geopolitical tension etc.); the ‘attribution problem’ (i.e. the ‘cyber-veil’) is therefore

⁴³ The concept of ‘cyberwar’ remains contentious primarily due to perception of what constitutes a ‘war’. For those who insist that a war can ‘only be waged with bombs and bullets’ cyberwar is an impossible concept. For those who accept that ‘war’ can also be applied conceptually (rather than legally) ‘cyberwar’ is more akin to ‘Economic War’ or even the ‘Cold War’, in that it represents a clear domain of ongoing state conflict where vital interests can be won or lost without resort to kinetic means.

⁴⁴ See Clarke, Richard and Knake, Robert K., *Cyber War: The Next Threat to National Security and What to Do about it*, New York, HarperCollins Publishers, 2010.

⁴⁵ See Sommer, Peter and Brown, Ian, *OECD/IFP Project on Future Global Shocks: Reducing Systemic Cybersecurity Risk*, 14 January 2011, <http://www.oecd.org/dataoecd/57/44/46889922.pdf>.

⁴⁶ Questions of the interdependency of Critical Infrastructure in general have been the subject of a number of studies conducted recently, mostly not however public. One such study is the so-called PIA-FARA Study with the wonderful title ‘1337 Critical Infrastructure Incidents in the European Union’. What effect Cyber-attacks can have on ICT infrastructure has been the subject of a number of different US and European Cyber-exercises, including the CYBERSTORM series and WHITE NOISE.

⁴⁷ Resilience is defined as ‘the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or man-made, under all circumstances of use’ (see O’Neill, Don, ‘Maturity Framework for Assuring Resiliency Under Stress’, *Build Security In*, 11 July 2007, <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/1016-BSI.html>).

⁴⁸ The school of ‘cyberdeterrence’ maintains that the best defence the US (or any nation) can have against cyberattack are strong offensive capabilities capable of inflicting unacceptable cost on any potential attacker (see, for example, Libicki, Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, Rand Corporation, 2009. http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf).

⁴⁹ See, for example, Corbin, Kenneth, ‘Obama’s Cyber Chief Touts ‘Resilient’ Security Strategy’, *eSecurity Planet*, 12 April 2011, <http://www.esecurityplanet.com/news/article.php/3892116/Obamas-Cyber-Chief-Touts-Resilient-Security-Strategy.htm>.

⁵⁰ See, for example, Kramer, Franklin D., ‘Cyber Conflict: Challenging the Future. Speech at the Black Hat Conference 18 January 2011’, *Atlantic Council*, 19 January 2011, <http://www.acus.org/news/franklin-kramer-us-should-aim-cyber-resilience>.

⁵¹ Doyle, 2011.

⁵² Ibid.

⁵³ See Libicki, 2009.

not of major concern.⁵⁴ This contention has increasingly been drawn into question, and has also partially led to a revision of the 'deterrence' position to include aspects of 'resilience', as expressed by US Deputy Secretary of Defence William Lynn: 'The challenge [of deterrence] is to make defences effective enough to deny an adversary the benefits of an attack.'⁵⁵

An essential commonality of both positions, and an underlying principle of any discussion on 'cyberwar', is the danger of inadvertent escalation of conflict in cyberspace. Due to the very rapid speed of action in cyberspace and the great potential for misunderstanding, either because of language use or because of ambiguous actions, great care has to be paid to prevent a rapid escalation of interstate tension. The effects could be dire.

1.5 International Law and 'Cyberwar'

Away from public view, discussions have been ongoing on how to classify state cyberattacks within an international legal framework.

Overall, the *jus ad bellum* question (i.e. when a cyberattack clearly constitutes an act of war) can be said to have been addressed: cyberwar could be said to occur when the 'level of damage inflicted was similar to an armed attack'.⁵⁶ Exactly what this means will, however, remain a point of contention in the future. As far as *cyber jus in bellum* is concerned, it is increasingly accepted that any cyberattack would have to conform to the major principles of the Law of Armed Conflict and International Humanitarian Law. Cyberattacks should be conducted with a distinction between military and civilian targets, consider the proportionality principle as well as the possibility of secondary and tertiary effects. What exactly this means (i.e. what ICT infrastructure could be considered purely civilian and what dual-use) is presently the subject of vigorous debate. A number of other issues, foremost the responsibility of nation-states to prevent third-party cyberattacks from being carried out from 'their' cyberspace (e.g. by non-state actors), has just recently begun to be discussed. Many in the West would consider that addressing this issue would represent a principle step in decreasing the potential for interstate cyberwar.

A different view on how de-escalation can be achieved is advanced by Russia (and to a lesser extent China). These countries would prefer to talk about state cyberweapons, and would treat these negotiations as essentially an arms-control issue, with treaties banning the 'development and deployment of cyberweapons'.⁵⁷ Most Western nations have traditionally considered such a treaty to be hardly enforceable and open to abuse, and have favoured instead the ratification of the Council of Europe Convention on Cybercrime as an important step to at least limit cyberattacks, including purported state-affiliated cyberespionage. The great increase of cyberespionage attacks against governments in 2009-2010 has prompted a compromise position – namely, culminating in deliberations on the 'Rules of behaviour' in Cyberspace.⁵⁸ A number of different organizations are currently engaged in 'one and a half' and 'second-track' diplomatic discussions on how this could best be achieved – without, however, notable EU representation on the issue.

⁵⁴ See *ibid.*

⁵⁵ See, for example, Lynn III, William J., 'Remarks on Cyber at the Council on Foreign Relations', *Crossroads*, 30 September 2010, <http://blog.cybersecuritylaw.us/2010/10/dep-def-sec-lynn-cyber-war-extends-conflict-93010.html>.

⁵⁶ This was agreed at the 'Cyber 15' deliberations conducted at the UN in the summer of 2010 (see PART 3: UN for more details).

⁵⁷ See Part 3.3. of this study.

⁵⁸ One of these initiatives is currently being developed by Eneken Tikk and others at the NATO CCD COE and is entitled '10 Rules of Behaviour for Cybersecurity'.

2 CYBERPOWER AND CYBERWARFARE CAPABILITIES

2.1 'Cyberpower' instead of Cyberwarfare?

War is a mere continuation of policy by other means

— Carl von Clausewitz,⁵⁹

Politics is the continuation of war by other means

— Michel Foucault,⁶⁰

Cyberwarfare as a concept has remained contentious, not the least because, for liberal democratic governments, the distinction between 'warfare' and mere 'attacks' is very important. 'We know what war looks like', a noted cybersecurity observer has said 'and it involves tanks and bombs.'⁶¹

This 'Western' binominal approach to state conflict has often been derided in Marxist-Leninist (or even post-modern) inspired thought. Some countries have indeed developed doctrinal concepts of interstate conflict that are active in times of both peace and war. The purported Chinese 'Information Warfare'⁶² concept (known as 'Three Warfare's') includes methods such as 'Legal Warfare' and 'Media Warfare' that might seem to be anathema to liberal democracies, yet certainly acknowledges the importance of 'Information' (broadly defined) in the so-called 'Information Age'. While liberal democracies cannot easily countenance such strategies and certainly do not see themselves in a constant state of war, it is clear that a higher-level paradigm is necessary, one that acknowledges the importance of the 'information domain' while not violating hallowed principles of liberal democracy. An equally important question is how to include the whole breadth of national cybersecurity issues in a paradigm that can encompass military and civilian cybersecurity issues, and function in times of both peace and war, and across the different components of 'national power'.⁶³

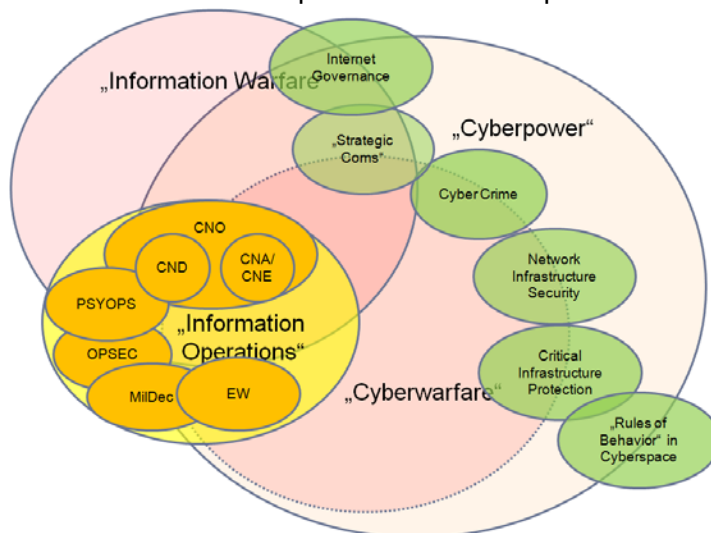


Image 1 Cyberpower - Themes

⁵⁹ Clausewitz, Carl von, *On War*, London, Penguin Books, 1982 [1832], p. 119.

⁶⁰ Foucault, Michel, *Society must be defended*, New York, Pan Books Limited, 2003 [1975-6], p. 15.

⁶¹ See also Shiels, Maggie, 'Cyber war threat exaggerated claims security expert', *BBC News*, 16 February 2011, <http://www.bbc.co.uk/news/technology-12473809>.

⁶² For a comprehensive study of the 'Three Warfare's Study' see Walton, Timothy, *Treble Spyglass, Treble Spear*, <http://www.c4ads.org/files/Three%20Warfare%202010.pdf>.

⁶³ Concepts of 'national power' refer to leverages of power of a nation-state or alliance; and can include different specific instruments. Most commonly these are referred to as including Diplomatic, Military, Informational and Economic (DIME) instruments.

What actually constitutes power in (and through) cyberspace is still poorly understood within the larger framework of national power, and the subject of much debate.⁶⁴ What is clear is that the 'cyberpower' of a nation does not necessarily derive solely from the amount of trained hackers it has, but rather the sum total of resources or capabilities it can leverage to support political goals. These include a great swath of capabilities and programs only marginally related to classical debates on cyberwarfare, such as Critical Infrastructure Protection (CIP) programs and Internet governance. A major portion of these cyber-capabilities is not subject to direct government control, and resides in the non-state (i.e. business and civil-society) sector. When examining the purported cyber-capabilities of a nation it is therefore necessary to have a wider view, to look at non-state capabilities as well as state capabilities, and to understand that these non-state capabilities are not always directly under state-control. The concept of cyberpower, especially when addressed through a capability-based approach,⁶⁵ is well suited to support this type of analysis.

2.2 China – Short Analysis⁶⁶

Few countries have concentrated on 'cyber' as much as China. In part this derives from the 'Gulf War shock' of 1991, in which the US military showed its total dominance in conventional warfare. Within this context, the Chinese military establishment has pursued cyberwarfare capabilities in an attempt to build an 'asymmetric counter' to this clear US military advantage in conventional warfare. Chinese military thought on the issue is generally considered to be at least as advanced as US and Western thought. The US is also seen as having the most advanced cyber-capabilities, and these are seen as a direct threat to China – China often proclaims itself to be the biggest victim of cyberattacks.⁶⁷ Further, China's explosive economic growth (to say nothing of the Internet itself) has profoundly affected the country. From the mid 1990s China has gone from around 1 million computers and virtually zero online communities to around 300 million computers and around 420 million Internet users in 2010.⁶⁸ This huge population of 'Netizens' ('people of the net') represents a major security concern for the Chinese Communist Party (CCP). Many of the Chinese cyber-programs are probably more concerned with 'co-opting' these potential subversives than with actual conflict with a foreign adversary.

China has very considerable cyber-resources. Besides the foreign spy agency MSS, most of the official Chinese offensive capabilities are probably concentrated in the military. The Chinese military capabilities are probably two-fold: at the strategic level, the PLA cyber-capabilities are purported to be concentrated within the (very large) General Staff Departments, and cover both strategic defensive and

⁶⁴ Cyberpower has been defined as 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power' (Kuehl, Dan, 'From Cyberspace to Cyberpower: Defining the Problem', in Kramer, Franklin D. et al. (ed.), *Cyber power and National Security* Washington, D.C., National Defence UP, 2009.). Starr and his colleagues, however, approach the issue primarily from a military perspective. A slightly broader view was offered by Joseph Nye, who considers the most important application of soft (cyber)power to be outward-facing, influencing nations, rather than inward-facing (see Nye, Joseph S., 'Cyber Power', *Harvard Kennedy School*, May 2010, <http://belfercentre.ksg.harvard.edu/files/cyber-power.pdf>).

⁶⁴ See Thompson, Mark, 'U.S. Cyberwar Strategy: The Pentagon plans to Attack', *Time*, 2 February 2010, <http://www.time.com/time/nation/article/0,8599,1957679,00.html>.

⁶⁵ One approach to understanding cyberpower is the Integrated Capability Model, which divides the cyberpower of a state into three dimensions: the ability to coordinate government action (Integrated Government Capability), the ability to collaborate with international partners (Integrated Systems Capability) and the ability to coordinate with the non-state sector (Integrated National Capability). See: Klimburg, 2011(a).

⁶⁶ See Appendix IV 'China: Military, Netizens and Patriot Hackers' for more details.

⁶⁷ See Lam, Willy, 'Beijing beefs up cyber-warfare capacity', *Asia Times*, 9 February 2009, <http://www.atimes.com/atimes/China/LB09Ad01.html>.

⁶⁸ See Internet World Stats, *China Internet Usage Stats and Population Report*, 2010, <http://www.internetworldstats.com/asia/cn.htm>.

offensive roles. At an operational level, the PLA has set up a large number of battalions that are integrated into military district and field-army structures. Some of these units probably directly support the operational capabilities of field units (as Western C4SIR units do), while others are perhaps officially intended as semi-autonomous militia units capable of waging 'strategic strikes' – i.e. attacking the enemies' critical infrastructure – on their own.

The latter 'strategic strike' militia units have been the subject of a vigorous discussion in the West. The PLA and the CCP are known to maintain a number of networks of non-state hacker groups, with the largest (for instance 'Red Hacker Alliance') claiming many tens of thousands of 'patriot hackers'.⁶⁹ It is often presumed that these networks are directly connected to these militia units referred to above, as they themselves are often based at universities or state-owned enterprises.⁷⁰ A large number of the cyberattacks that have been reported on in the West are thought to have originated from this group. However, these are not necessarily the most damaging or sophisticated of attacks (also known as APT – Advanced Persistent Threats, such as the ca. 2003 'Moonlight Maze' attacks); many of these are probably still conducted by 'official' state chackers in addition to the patriot hackers' campaigns. The non-state activities do complement possible 'official' cyberattacks by increasing the overall strain on the targeted countries' cyberdefences.

Overall, it is likely that Chinese cyberattacks encompass non-state and state-directed activity – the former can be quite 'noisy' and obvious, while the later is usually of a much higher technical standard.⁷¹ Both categories of attack represent a significant challenge to the EU, particularly regarding Advanced Persistent Threats – i.e. cyberespionage. Patriot hacker attacks are usually 'highly opportunistic' both in terms of their initial targeting and probable connection to the government; the majority of these non-state hacker groups probably do not have regular operational connection to the Chinese security services. It is unclear if the non-state patriot hacker attacks are primarily a result of an encompassing government strategy to attack foreign information systems, or if they simply represent a 'make work' strategy to keep these potential subversives occupied. By 'co-opting' these non-state actors into supporting state policy the government might mainly be seeking to prevent the 'patriot hackers' from attacking the state itself.

2.3 Russia – Short Analysis⁷²

The Russian focus on Psychological Warfare (PSYWAR) goes back many decades and plays an important role in understanding Russian concepts regarding Information Warfare and cyberpower. In general, Russian strategic thought sees PSYWAR as a conflict-winning paradigm, one that can directly undermine Russian security not only using 'Information-Technical' means (e.g. cyberattack), but also 'Information-Psychological' attacks. The latter can be construed, in some cases, to include 'harmful' criticism of the government. Russia has long been acutely concerned that the US 'hegemony' on the Internet provides for a number of advantages to the US in both attack categories, to Russia's detriment. As a reaction to this, Russia has long considered it important to seek to expand its influence within Internet governance as a whole, and to diminish the perceived influence of the United States. On an operational level it has started the development of its own PC operating system (similar to China), and

⁶⁹ See Minnick, Wendell, 'Is Beijing Behind Cyberattacks on the Pentagon?', *DefenceNews*, 2 June 2008, <http://www.defencenews.com/story.php?i=3576373&c=FEA&s=SPE>.

⁷⁰ See Thomas, Timothy L., 'Comparing US, Russian, And Chinese Information Operations Concepts', *Foreign Military Studies Office*, February 2004, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf.

⁷¹ US-China Economic and Security Review Commission, *China's Propaganda and Influence Operations, its Intelligence Activities that Target the United States and the Resulting Impacts on U.S. National Security*, 30 April 2009, http://www.uscc.gov/hearings/2009hearings/transcripts/09_04_30_trans/09_04_30_trans.pdf.

⁷² See Appendix V 'Russia: Siloviki, Cybercrime and Hacker Patriots for more details'

has even gone as far as actively considering developing its own search engine to replace Google,⁷³ which is seen as being 'American'.

Within the government itself, the strength of the security services has meant that former ties to organised crime (which were common in the 1990s) might still play a role in governmental cybersecurity. Russia itself has produced a wide number of talented programmers, which has contributed not only to political hacktivism ('hacker patriots'),⁷⁴ but most importantly to the rise of Russian cybercrime. Russian cybercrime is dominant worldwide – in 2007 up to 40% of global cybercrime was related to only one Russian cybercrime gang. These considerable non-state resources are probably regularly utilized by Russian government for 'Information-Technical' purposes.⁷⁵ Overall, the Russian government and its intelligence services maintain a number of different methods to encourage or 'coerce' non-state actors into collaboration with state authorities.⁷⁶

Russian state cyber-resources are largely not public, but are presumed to be overwhelmingly based within the intelligence services, rather than the military directly. The dominance of the (ostensibly internal-security) FSB⁷⁷ among the intelligence services themselves has led to the assumption that the FSB also plays a key role in CNE attacks abroad. The Russian government has a number of direct and indirect means to 'encourage' (or 'coerce') the cooperation of the non-state sector. At the top level, a number of so-called Kremlin-affiliated businesses have been active in purchasing shares in online media companies at home and abroad, among others in 'Facebook' and ICQ. Lower down, virtually all ISPs in Russia are de-facto required to follow the stipulations of the SORM legislation, which in effect gives the intelligence service the ability to monitor most (if not all) Internet traffic occurring within Russia. Finally, suspected cybercriminals have very often avoided prosecution in Russia, sometimes even reappearing in government advisory positions. It is also known that local FSB offices or cross-departmental organizations headed by the FSB have actively tried to recruit Russian hacker-patriot to wage attacks, usually on foreign enemies.⁷⁸

The Russian 'hacker patriots' are not nearly as active as Chinese 'patriot hackers' (in particular as far as APT is concerned), but often seem to be more closely connected to the government. In some cases (in particular the Georgian 2008 attacks) there was clear coordination between supposedly non-state hacker patriots and the armed forces.^{79,80} Since the relatively high-profile attacks on Estonia 2007 and Georgia 2008, among others, there have been only few major incidents of Russian hacker patriots attacking foreign countries. At the same time, Russian cyberespionage, either directly criminal or state-directed, has increased.

⁷³ Open Source Center, *OSC Report: Russia – Russia Cyber Focus*, 7 May 2010, Issue, <http://publicintelligence.info/OSC-RussiaCyberFocus9.pdf>.

⁷⁴ See Klimburg, Alexander, 'Mobilising Cyber Power', *Survival*, vol. 53(1), 2011(a), p. 41-60.

⁷⁵ Bikkenin R., 'Information Conflict in the Military Sphere: Basic Elements and Concepts', *Morskoj Sbornik*, no. 10, 2003 (translated in Highbeam).

⁷⁶ See Appendix V for examples

⁷⁷ Agentura, *Structure of the FSB*, <http://www.agentura.ru/english/dosie/fsb/structure/>.

⁷⁸ See Rainsford, Sarah, 'Inside the Mind of a Russian Hacker', *BBC News*, 11 March 2010, <http://news.bbc.co.uk/2/hi/8561910.stm>; and Walker, Shaun, 'Was Russian Secret Service Behind Leak of Climate Change Emails?', *The Independent*, 7 December 2009, <http://www.independent.co.uk/news/world/europe/was-russian-secret-service-behind-leak-of-climatechange-emails-1835502.html>. The release of the e-mails was probably timed to influence the 2009 Copenhagen climate summit, and the stolen archive was disseminated by uploading to a server in Russia. The question of FSB involvement, however, is speculative.

⁷⁹ See Project Grey Goose, 2009.

⁸⁰ See US-CCU, 2009.

2.4 United States – Short Analysis⁸¹

The United States effectively invented the Internet, and US-based institutions dominate much of what constitutes world-wide cybersecurity. Within the military, the United States was the first country to actively seek to leverage ‘Information dominance’, and since the early 1990s has steadily expanded its doctrine of Information Operations (IO). Due in part to its electronic warfare heritage within the US Air Force, IO thought is mostly concentrated on supporting conventional military operations (such as ‘suppression of enemy air defence’) and less focused on the possible cyberwar capabilities of strategic strike (as it is in China) or psychological warfare (as in Russia). An even more important determinant of overall US cybersecurity capabilities is, however, the US Constitution.⁸²

The United States federal government (i.e. not including state governments) probably spends more on cybersecurity than the rest of the world combined.⁸³ The US maintains a very large number of cyber-organizations, the majority of them within the military, and most of them concerned with purely defensive tasks. For the US military, as well as for most Western military establishments, communication networks have become absolutely essential for the conduct of ‘Network Centric Warfare’, and the defence of these increasingly elaborate networks requires substantial resources. Most of the few identifiable US cyberattack organizations probably focus on ‘operational-level’ IO; and the ability to support conventional military operations, rather than ‘strategic strike’.

Even more than most EU Member States, the US faces numerous constitutional challenges to effective cybersecurity. US Code clearly assigns responsibility for various tasks (such as ‘domestic security’, ‘armed forces’ etc.) and this can make it difficult for some parts of the US government to cooperate with others. Until recently (2010) effective cyber crisis-management in the US was largely dependent on the ‘identity of the aggressor’, something that would probably have been difficult to determine at the time of an attack. The US has however recently advanced considerably in its ‘Whole of Government’ cybersecurity capabilities. The new National Cyber Incident Response Plan (and relevant organizations such as NCCIC⁸⁴) was a major step forward, and did for civilian cyberdefence (DHS⁸⁵) what the establishment of USCYBERCOM (DoD⁸⁶) did for cyberattack and military cyberdefence. The DHS and DoD have recently started to cooperate on ‘homeland defence’ missions,⁸⁷ although even these very tentative first steps have been heavily criticized for leading to a ‘militarization’ of cyberspace. Overall, the US has traditionally been comparatively weak on ‘resilience’ and has sought to compensate with ‘deterrence’. The recent advances of US (civilian) cyberdefence in building-up ‘resilience’ has also meant that within the Defence Department there is an increasing understanding that longer-term strategies of

⁸¹ See Appendix VI ‘The US: InfoOps, Private Business, and ‘White Hats’’ for more details.

⁸² US (federal) Cyber-capabilities are heavily segmented according to tasks assigned in Title 6 (Domestic Security), Title 10 (Armed Forces), Title 18 (Crimes and Criminal Procedure), Title 32 (National Guard), Title 40 (Public Buildings, Property, and Works), and Title 50 (War and National Defence) see NSMC-CO Appendix A 1, <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf>.

⁸³ Based on assessments of US Defence spending as well as calculations of current US cybersecurity expenditure (see Appendix VI for details; for US Defence spending see Shah, Anup, *World Military Spending*, 7 July 2007, <http://www.globalissues.org/article/75/world-military-spending>).

⁸⁴ National Cybersecurity and Communications Integration Centre (NCCIC) – a large, 24-hour, DHS-led coordinated watch and warning centre with particular national cyberdefence crisis management tasks.

⁸⁵ The Department of Homeland Security (DHS) is responsible for the protection of the ‘.gov’ domain and has the lead in coordinating most Critical Infrastructure Protection programs.

⁸⁶ USCYBERCOM is a shared US STRATCOM (Department of Defence) and NSA (National Security Agency) organization that besides cyberattack/-espionage is also responsible for general defence of the ‘.mil’ domain as well as protecting private-sector contractors. Although functionally independent of the DoD, the NSA has always officially been part of the DoD.

⁸⁷ See Chabrow, Eric, ‘DHS, DoD to Tackle Jointly Cyber Defence’, *Government Information Security*, 14 October 2010, http://www.govinfosecurity.com/articles.php?art_id=3010.

cyberpower will have to be based more on 'governance' theories of cooperation and national power than on nuclear-era defined concepts of deterrence. This especially applies to the overall importance of the non-state sector, cooperation with which only can be addressed through models of governance.

2.5 Assessment

As in most EU Member States, the majority of US cybersecurity and cyberpower capabilities are not governmental, but non-state.⁸⁸ The private sector is responsible for virtually all of the software and hardware that is exploited in cyberattacks, maintains most of the network infrastructure where these attacks are conducted, and often owns the critical infrastructure that these attacks are directed against. Further, civil society actors – as distinct from the private sector – dominate cyberspace, defining the programmed parameters (i.e. the software protocols) of the cyberdomain, as well as executing, researching and ultimately publicly speculating on cyberattacks.⁸⁹ Together, these non-government actors account for the bulk of what is termed 'national' cybersecurity. The involvement of these vital actors in comprehensive national cybersecurity has only just begun.

With the notable exception of Critical Infrastructure Protection (CIP) programs and security contractors, liberal democracies (as well as most EU Member States) have interacted relatively little with the non-state cybersecurity capabilities – a very wide, and absolutely vital, component of cybersecurity and cyberpower. Russia and China have in many ways progressed much further in seeking the cooperation of their non-state cyber-capabilities in national cyber policy, even if these capabilities are actually less important in these respective countries than the state capabilities are. The situation is probably reversed in liberal democracies – here the non-state sector is more important than the state sector in generating overall cybersecurity. A major challenge seems to be that while more restrictive forms of government can co-opt or coerce cooperation from their non-state sector, most liberal democracies can only aim to convince their non-state sector of the merits of cooperation. This requires, in effect, a new approach to government, a rethinking of the role of the non-state sector in security, and perhaps even a new appreciation of the implicit strengths of liberal democratic systems.

⁸⁸ Priest, Dana and Arkin, William M., 'A Hidden World, Growing Beyond Control', *Washington Post*, 19 July 2010, <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>.

⁸⁹ Borsook, Paulina, 'How Anarchy Works – On Location with the Masters of the Metaverse, the Internet Engineering Task Force', *Wired*, October 1995, <http://www.wired.com/wired/archive/3.10/ietf.html>.

3 INTERNATIONAL ASPECTS OF CYBERSECURITY

3.1 Internet Governance and Cybersecurity

Cyberspace only exists within parameters constructed and regulated by human beings. These parameters have, until now, not been created directly by governments, but have rather arisen from the 'bottom-up' in a process that is often referred to as the self-regulation of the Internet.⁹⁰ The process is often transcribed as 'Internet governance', which has been defined as 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.'⁹¹

The Internet is a relatively new environment for human activities, and was created with other purposes in mind than that for which it is now used. The basic Internet was never intended to be 'secure'; security was always more of an afterthought than an original design feature – in essence, the DNA of the Internet was to be a 'trusting, open' system. It did not appear feasible twenty years ago that not only would critical infrastructures partially come to depend on the Internet, but the Internet itself would be (at least in part) considered critical for everyday societal needs. Internet governance can therefore be considered not only a young, highly dynamic but also an essentially reactive policy field that seeks to reconcile the technical and policy heritage of the Internet with its ever-growing modern-day importance. Governments as a whole have been relative late-comers to Internet governance, despite its obvious political importance. The EU has considerable potential to play a formative role in evolving Internet governance, and help promote the development of a more secure Internet.

3.1.1 Technical Internet Governance: ad hoc

Internet governance can be subdivided into two domains: the technical and the policy domain. The technical domain is widely dominated by volunteers and the civil society and can be described as completely 'ad hoc'. One of the most important is the **Internet Engineering Task Force (IETF)**, which has, since 1986, developed many of the key software protocols and technical fixes that the Internet depends upon today. The IETF is famously anarchic, not having any official laws, membership criteria or indeed much more than a basic organization. The members of the IETF '*reject Kings, Presidents and voting. We believe in rough consensus and running code*'.⁹² Meeting (usually) three times a year, the 300 to 1,300 software engineers don't vote on proposals. Instead, they hum. Whichever group is perceived to have 'hummed louder' carries the (non) vote.⁹³ Other groups, such as the **Institute for Electrical and Electronics Engineers (IEEE)**, are more organized, but work in a similar 'bottom-up' approach with absolutely minimal governmental influence. The IEEE has over 350,000 members and addresses issues regarding connectivity (such as Bluetooth, Wireless and broadband). Groups such as the IETF and the

⁹⁰ See, for example, Ang, Peng Hwa, 'Self Regulation after WGIG', in Drake, William J. (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, New York, UNICTTF, 2005, pp. 129-34, <http://www.wgig.org/docs/book/toc2.html>; for a shorter and older bibliography that provides a good overview of uses of the term, see Internet Law and Policy Forum, 'A Bibliography of Internet Self-Regulation', undated, http://www.ilpf.org/events/selfreg/bib4_18.htm.

⁹¹ WGIG, 'Report of the Working Group on Internet Governance', *Château de Bossey*, June 2005, p. 4, <http://www.wgig.org/docs/WGIGREPORT.pdf>.

⁹² Attributed to Dave Clark: see, for instance, in Borsook, 1995.

⁹³ The IETF is in its very existence 'unofficial' – it does not legally exist, and is officially part of the Internet Society (ISOC) – itself one of the 'founding organisations' of the Internet.

IEEE can justifiably claim to have built the Internet, one protocol at a time. Governments have mostly played only a supportive role in this process.

3.1.2 Policy Internet Governance: institutionalized

The policy 'domain' of Internet governance is considerably more organized. **ICANN, the Internet Corporation for Assigned Names and Numbers** is the one organization that comes closest to having an assigning, coordinating or regulating function (and especially a policy function) on the Internet. ICANN is a 'nonprofit public-benefit corporation', according to the laws of the US State of California, and is based at the University of Southern California. Its purpose is to 'coordinate, at the overall level, the global Internet's systems of unique identifiers'.⁹⁴ Founded in 1998 on the basis of preexisting technical organizations, ICANN was the direct result of President Clinton's promise to move the Internet out of the government structures⁹⁵ and to open it to the public and to private commerce. Under a contract with the US Department of Commerce, ICANN was to 'manage Internet names and addresses', a relatively innocuous-sounding mission that encompasses three of the most vital functions of the Internet: the allocation of Internet Protocol (IP) number resources for individual computers or machines, directly corresponding to these, Domain Name Service (DNS) 'names', and the allocation of the so-called Top Level Domains (TLDs)⁹⁶ to 'registries' that actually assign these identifiers to individual users and organizations across the globe. Taken together, these three functions represent a considerable segment of Internet functionality.

ICANN has grown with the Internet⁹⁷ - from a marginal budget in 1999 to USD 60 million in 2010. Its nature has changed considerably as well. On the one hand, governments have shown increasing interest in the formative work of ICANN, and the **Government Advisory Council (GAC)** has become especially active. While ICANN was 'released' from US government control in October 2009, the US government still retains significant influence - more than other countries represented on the GAC. The increased interests of governments in ICANN, the rise in relative strength of national and generic 'registries', technical developments as well as the general 'need for a mission' has meant that ICANN has increasingly positioned itself as a security actor. This is especially evident in the roll-out of **DNSSEC** (the new DNS protocol of the Internet), which is one of ICANN's main functions. Furthermore, the increasing likelihood of attacks on the core infrastructure of the Internet (e.g. DNS and BGP Protocols) has made a case for the establishment of a **global DNS CERT** - a role that ICANN is very interested in taking on. However, the International Telecommunications Union (ITU) has showed great interest in assuming this role as well.

The **ITU** has often sought to challenge ICANN's position as the principal body in Internet governance. As a UN-agency, it has played a key role in many of the UN initiatives in cyberspace, including helping to organize the **Internet Governance Forum (IGF)** and the **World Summit of the Information Society (WSIS)** Process. The IGF has become an annual event for the global stakeholder community, where governments, private sector stakeholders and other interested groups present their views and proposals for Internet-related issues. The ITU has mainly contributed to Internet governance within the

⁹⁴ See, for instance, ICANN, *Bylaws*, 25 January 2011, <http://www.icann.org/en/general/bylaws.htm>.

⁹⁵ See, for instance, Mueller, Milton, 'Dancing the Quango: ICANN and the Privatization of International Governance', *Conference on New Technologies and International Governance*, 11-12 February 2002, <http://faculty.ischool.syr.edu/mueller/quango.pdf>.

⁹⁶ There are a number of different TLDs. The 'generic Top Level Domains' (gTLD) include all Internet addresses that, for instance, end with .com, .org, or .info. National domains are known as 'country code Top Level Domains' (ccTLD) and, for instance, end with .de, .fr, or .uk.

⁹⁷ See Klimburg, Alexander, *Ruling the Domain - (Self) Regulation and the Security of the Internet*, 2011(b), www.oijp.at (unpublished).

technical domain. An ITU High Level Expert Group on Cybersecurity was established in 2007. It serves as a consultation forum for information security experts from different regions and produces reports on cybersecurity. It has also sought to promote its own dedicated cyber-centre, **IMPACT**, located in Malaysia. In 2008, the controversial ITU-T Resolution 69⁹⁸ on 'Non-discriminatory access and use of the Internet resources' effectively called for an 'internationalization' of the Internet and was principally backed by Arab states, Russia and China. Around the same time, ITU Secretary General Touré referred to participation in ICANN's GAC as a 'waste of time' – he has often indicated that the 192-memberstate ITU 'family' was a more appropriate forum for many of the looming global issues in cybersecurity.⁹⁹ While the EU initially was a strong supporter of the ITU in calling for a better 'internationalization' of Internet governance, it also welcomed the US decision to 'free' ICANN¹⁰⁰ in 2008, and acknowledged that a significant step had been taken.¹⁰¹ Recently, a number of EU Member States have been much less active in supporting ITU's ambitions. In a landmark summit in Guadalajara, Mexico, in October 2010, these countries joined the US and other OECD nations in limiting an expansion of the ITU's role in Internet governance.

National governments have shown a growing interest in Internet governance. What was previously described as operating under a '**multi-stakeholder model**' (governments, private cooperation and the civil society) is coming under increased pressure from national governments who are trying to expand their relative importance in domain at the expense of the other stakeholders, according to some academics.¹⁰² The GAC is also trying to upgrade its importance to a body that can influence decisions of the ICANN board – interestingly, the present US proposal to this mirrors one European delegates made in 2005 that was blocked by the Bush administration. The Internet Governance Forum is also attempting to redefine itself as part of the renewal of its five year mandate – a redefinition process that governments initially tried to reserve for themselves as their own prerogative. However, as the ITU General Meeting showed, there is still substantial support for the multi-stakeholder approach, and signs that Western OECD nations in particular are joining together to support it.

3.1.3 Informal International Cybersecurity Initiatives

In addition to formal initiatives in Internet governance, a number of very well-established informal forums exist in the cybersecurity field. These informal processes (sometimes even initiated by governments) have often been more efficient than many top-down processes led by international organizations. Trust-based information security experts' networks have shown their ability to mobilize the needed expert knowledge and networks in most international cybercrises so far. Governments and international organizations should consider maintaining the positive aspects of these informal networks when designing more formal cooperation and coordination mechanisms.

In the policy domain, one of the foremost groups is the **Meridian forum for global critical information infrastructure protection (CIIP)**¹⁰³. It publishes the only regularly updated global

⁹⁸ See ITU, 'Resolution 69 – Non-discriminatory access and use of Internet resources', *World Telecommunication Standardization Assembly*, Johannesburg 21-30 October 2008, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.69-2008-PDF-E.pdf.

⁹⁹ See New, William, 'Controversy Over Internet governance: ITU Families And ICANN Cosmetics?', *ITU*, http://www.itu.int/osg/csd/intgov/ituinpress/new_william.html.

¹⁰⁰ From the Joint Project Agreement (JPA) that effectively made ICANN subordinate to the Secretary of Commerce

¹⁰¹ See Rapid Press Release, *European Commission welcomes US move to more independent, accountable, international Internet governance*, 30 September 2009, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1397>.

¹⁰² Including comments made by Victor Mayer-Schönberger of the Oxford Internet Institute at a recent conference in Vienna (see <http://www.domainpulse.de/de/programm>).

¹⁰³ A generic term used for all vital information and communication technology (ICT) services and infrastructures is Critical Information Infrastructure (CII). All the civilian efforts in advancing cybersecurity by focusing on prevention, preparedness

reference book for national cyber-systems, or CIIP policies, as well as maintains Points of Contact for cyber-emergencies in more than 50 countries. Meridian has annual and regional events and serves as a major global trust-building and consultation forum for cybersecurity policies. The Meridian members also issue recommendations, share best practices, offer IT security standard setting guidelines, and other information for its participants.

Within the technical domain, **FIRST (Forum of Incident Response and Security Teams)** is one of the most important communities for Internet and network security experts. At FIRST conferences IT security specialists exchange information and experience in incident -handling practices, and build the personal contacts that can be crucial in times of crises. Within the working groups and similar expert forums, the specialists deliver many of the key protocols and build informal networks that information security have grown to depend upon. FIRST also accredits CERTs worldwide, i.e. confirms that they have bona fide processes, and therefore plays a crucial role in helping to harmonize national cybersecurity efforts.

3.2 International Multilateral Organizations and Cybersecurity

One of the major instruments in enhancing international cybersecurity is the **2001 Council of Europe Convention on Cybercrime**. It provides guidance on how national legal frameworks should be harmonized and on the elements of international cooperation in fighting cybercrime. Currently, the Convention has 47 signatory countries, of which 30 have also ratified the convention. Of the remainder, the majority has not yet ratified but has nonetheless already implemented the Convention. The importance of this legal instrument is both practical and political. As it sets guidelines for developing respective national legal frameworks against cybercrime, it is a useful tool for 'exporting' European norms on the issue. Furthermore, accession to the Convention also facilitates international cooperation on operational matters – including extradition of cybercriminals. The political importance of the Convention lies in the fact that it is the only binding international agreement on cybersecurity issues, and accession to the Convention shows that a country is ready to harmonize its internal laws and to take the fight against cybercrime seriously. The Council of Europe, together with the private sector and Member States, has launched a Global Project on Cybercrime¹⁰⁴ to promote the Convention worldwide. As a result of this initiative, many countries outside Europe, especially in Asia and Latin America, have drawn on the Convention's example and have implemented legislative reforms.¹⁰⁵ Not only will the success of the fight against cybercrime in developing countries affect the economic, internal and international security of the EU, but also the EU countries will benefit from a wider acceptance of the Convention's principles beyond the EU. The increasing number of countries joining this Convention provides for a significant deterrence to criminal groups and governments sponsoring cyberattacks via proxies on their territories.

The Organization of Economic Cooperation and Development (OECD) intergovernmental Working Party on Information Security and Privacy (WPISP) develops policy recommendations and reports on the information society and resilience building. Through its network of experts from government, business and civil society, it monitors trends and facilitates information exchange. The OECD issues

and resilience building of the CII fall under the common generic concept Critical Information Infrastructure Protection (CIIP). The common terminology has yet to emerge in the field of cybersecurity, but most of the EU institutions have started to refer to Critical Information Infrastructures (CII) in official policy documents as '*ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures*'.

¹⁰⁴ Global Project on Cybercrime on Council of Europe website: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/projectcyber_en.asp.

¹⁰⁵ See Council of Europe, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

regular reports analyzing the impact of technology on information security and privacy. The OECD report on CIIP practices among its Member States is one of the best comparative documents in the field, comprising analyses of best practices, organizational structures and the regulations of the most advanced economies.¹⁰⁶ Recently, the OECD started a research series on 'Global Shocks' with a report on 'Reducing Systemic Cybersecurity Risks'¹⁰⁷ – the authors arguing that it would require a 'perfect storm' for cyberattacks to have debilitating consequences on national infrastructures. As cybersecurity in the OECD context has predominantly been a sub-category of economic and technology policy, the rise of cybersecurity as a subject for national security has somewhat reduced its importance for the OECD's agenda. However, the OECD's contribution to collecting and exchanging the best practices in building national information infrastructure resilience¹⁰⁸ could be useful for those EU Member States who are still searching for the right model for their respective national cybersecurity organizations – which many Member States indeed are.

The Organization for Security and Cooperation in Europe (OSCE) started discussions on cybersecurity in 2008, with support from the Estonian Chairmanship of the Political and Security Committee.¹⁰⁹ Since then, the states participating in the OSCE have held several high level meetings on cybersecurity, where central themes of the discussions have included raising cybersecurity awareness, a need for countries to build their capability to fight against cybercrime and terrorism, as well as determining responsible state behavior in cyberspace. OSCE countries have very different interests and angles in approaching the subject of cybersecurity, and consensus has not emerged on what the exact role of the OSCE will be in the debate. The Joint Meeting of the OSCE Forum for Security Cooperation and the OSCE Permanent Council held in June 2010 decided that discussions will continue on strategic cybersecurity issues. The U.S. proposed a discussion on norms for state behavior in cyberspace in 2010.¹¹⁰ At the same time, the Russian position was to develop a universal cyber-convention, while not specifying what this new document would include.¹¹¹ Overall, instead of a cyber-convention, some Western nations have started to back calls for 'norms on acceptable state behavior in cyberspace'.¹¹² The idea had been circulating for some time in the international legal and policy community¹¹³ before being supported by the US. As many governments have also started to see the value in this approach, the OSCE may be an appropriate organization for discussing international cyber-norms in a wider

¹⁰⁶ See OECD, *Development of Policies for Protection of Critical Information Infrastructures. Ministerial Background Report (DSTI/ICCP/REG(2007)29/FINAL)*, 17-18 June 2008, <http://www.oecd.org/dataoecd/25/10/40761118.pdf>.

¹⁰⁷ See Sommer and Brown, 2011.

¹⁰⁸ 'Resilience' is understood as an ability of the infrastructures to function reliably under conditions of uncertainty. The reliable management of the infrastructure organizations is in compliance with certain set of procedures and standards that guarantee the resilience. There are three components which will form resilience of national critical infrastructures in following categories – physical, organizational and technological aspects of organization's security practices. Cybersecurity is concerned with the latter category, but not exclusively. Because of the interlinking of all these categories they are part of the risk management process of any organization and need to be mutually supporting. For example, the most advanced cybersecurity technology is helpless if the door to the server room is left open to the intruders.

¹⁰⁹ See OSCE Press Release, *OSCE can play important role in cyber security, says Estonian Defence Minister*, 4 June 2008, <http://www.osce.org/fsc/49775>.

¹¹⁰ See Schneider, Deborah, 'Cyber Security Keynote Address for the U.S. Department of State', *United States Mission to the OSCE*, 9 June 2010, <http://www.osce.org/fsc/68524>.

¹¹¹ Statement by Mr. Shestakov at the Joint Meeting of the OSCE Forum for Security Cooperation and the OSCE Permanent Council, FSC-PC.DEL/30/10 9 June 2010 <http://www.osce.org/fsc/68693>.

¹¹² Most recently, British foreign secretary William Hague has called for rules of behavior in cyberspace and the promotion of international norms at the Munich security conference in February 2011 (see <http://www.telegraph.co.uk/news/politics/william-hague/8303806/William-Hague-proposes-cyber-warfare-rules.html>)

¹¹³ CCD COE *Proceedings of the NATO CCD COE Conference on Cyber Conflict*, Tallinn July 15-18 2010, <http://www.ccdcoe.org/conference2010/>.

multilateral framework, despite the obvious drawback of not having the world's largest cyber-nation, China, as a participating state.

3.3 United Nations and Cybersecurity

The **UN General Assembly** has agreed on a number of resolutions relevant to cybersecurity. Under the **UN Social and Economic Committee** resolutions 56/121 'Combating the Criminal Misuse of Information Technology'¹¹⁴ and 57/239 'Creation of a Global Culture of Cybersecurity'¹¹⁵ were adopted. Both resolutions stress the importance of international cooperation, the need to eliminate safe havens for cybercriminals, to encourage law enforcement cooperation, as well as to enhance general awareness of cybersecurity issues. Resolution 64/422 'Globalization and interdependence: science and technology for development'¹¹⁶ also included the CIIP self-assessment survey for UN countries to advance their cyber-protection. These initiatives have drawn attention to rising concern over cyber-threats and helped to raise global awareness as well as encouraged UN countries to adopt the necessary measures to advance their national mechanisms for cybersecurity.

Under the **UN Disarmament Committee**, UN resolution 64/386 'Developments in the field of information and telecommunications in the context of international security'¹¹⁷ was adopted in 2009. The resolution proposed to continue discussions on cybersecurity in the context of international security and to convene a group of experts that would issue further recommendations. In 2010 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security¹¹⁸ produced a report that calls on countries to collaborate to improve information security and international cooperation. The report offers recommendations for further dialogue among states to reduce risk and protect critical national and international infrastructures.¹¹⁹ The **2010 UN report on cybersecurity** is an important milestone in framing the cyberwarfare issue within currently existing international law. The question that international lawyers and governments have investigated for some time, namely the applicability of current international law instruments in cyberspace, was tackled in the process of preparing the report. The negotiations led participating countries to agree that the major principles of the Law of Armed Conflict and International Humanitarian Law also apply in cyberspace.¹²⁰ Once cyberattacks reach the threshold of an armed attack, they need to follow the agreed rules of conducting warfare. This approach solves the *jus in bello* question of cyberwarfare. It states that cyberattacks should be conducted in a manner that make a distinction between military and civilian targets, consider the proportionality principle as well as the secondary and tertiary effects. Cyberwarfare needs to prohibit attacks that are not restricted to military objectives. The *Jus ad bellum* question in cyberwarfare, as to when the cyberattack reaches the

¹¹⁴ UNGA, *Combating the Criminal Misuse of Information Technology*, A/RES/26/121, 23 January 2002.

¹¹⁵ UNGA, *Creation of a Global Culture of Cybersecurity*, A/RES/57/239, 31 January 2003.

¹¹⁶ Globalization and interdependence: science and technology for development
<http://www.un.org/esa/coordination/globalization.htm>.

¹¹⁷ UNGA, *Developments in the field of information and telecommunications in the context of international security*, A/64/386, 2 July 2007.

¹¹⁸ UNGA, *Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/94, 24 June 2010.

¹¹⁹ The report also confirms that nation states are increasingly developing the instruments of cyberwarfare. In addition to states, individuals and criminal organisations are likely to use these disruptive tools or act as proxies. The report highlights also the possibility of terrorist groups using disruptive ICT tools in the future. The report offers specific recommendations on reducing the global risks originating from malicious exploitation of cyber tools, including further dialogue to reduce collective risk, exchange of best practices, support for capacity building in less developed countries and enhancing stability by other cooperative measures.

¹²⁰ See Schneider, 2010.

threshold of an armed attack, is far more difficult to determine. The UN charter framework and the principle of self-defence apply if cyberattacks have caused damage comparable to the consequences of an armed attack.¹²¹

3.4 NATO Cyberdefence Initiatives

After the 2007 attacks against Estonia, NATO developed its first Cyberdefence Policy, which constitutes the basis for other strategic documents and activities in the field.¹²² NATO was the first international organization to adapt quickly to the new strategic environment, and recognized that non-traditional security threats are central to the national security of the Allies. NATO's 2007 Cyber Defence Policy set objectives for bolstering the cyberdefence capabilities of NATO's own networks, and established initial mechanisms for consultations with Member States in cyberdefence issues.

The **NATO Cyber Defence Management Authority (CDMA)** Board has the main responsibility for coordination and strategic decision-making on cyberdefence within the Alliance. The newly established **Emerging Security Challenges Division** coordinates political and strategic oversight for NATO cyberdefence efforts. The **NATO Computer Incidence Response Capability Technical Centre** serves as a central technical authority on operational cyberdefence issues. In order to promote consultations among Member States, NATO has initiated a framework of Memoranda of Understandings with Allies. The cyberdefence MOU-s between the NATO CDMA and national cyberdefence authorities facilitate regular consultation, information -sharing, and describe how the NATO **Rapid Reaction Teams** can support individual Allies in case of cybercrises.¹²³

The new **NATO Strategic Concept** adopted at the Lisbon Summit in November 2010 stresses that NATO must accelerate efforts to respond to the danger of cyberattacks.¹²⁴ The concept also states that NATO should bring all of its agencies together under a protective umbrella and to include the cyber domain in its defence-planning process. NATO seeks to support Allies to prevent attacks and to recover from them, and in the development of additional cyberdefence capabilities. The long-debated issue of whether NATO's Article V applies in Cyberspace is also indirectly addressed in the Strategic Concept, where NATO reiterates the principle of collective defence for all categories of threats. 'NATO will deter and defend against any threat of aggression and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole'.

The **Lisbon Summit** commits NATO and the Allies to address the new security challenges and, among other objectives, draws a very ambitious roadmap for the cyber-agenda of the Alliance. It includes bringing all NATO military and civilian bodies under central protection, introducing the cyber-component to the defence planning process and accelerating information sharing and early warning capabilities.¹²⁵ NATO will adopt a new cyberdefence policy by June 2011.¹²⁶

¹²¹ For further reading on the debate refer to Carr, Jeffrey, *Inside Cyber Warfare. Mapping the Cyber Underworld*, Beijing et al., O'Reilly Media Inc., 2010, chapter 3.

¹²² See NATO, 'Defending against cyber attacks', *NATO A-Z*, 18 March 2011, http://www.nato.int/cps/en/natolive/topics_49193.htm.

¹²³ See *ibid.*

¹²⁴ See NATO, *Active Engagement, Modern Defence*, 19 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

¹²⁵ See NATO, *Lisbon Summit Declaration*, 20 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm?selectedLocale=en.

¹²⁶ See NATO, *Developing NATO's cyber defence policy*, 25 January 2011, http://www.nato.int/cps/en/natolive/news_70049.htm.

NATO's Centre of Excellence on Cooperative Cyberdefence (CCD COE), situated in Estonia, aims to develop the following fields in cyberdefence: training and education, research and development, legal and policy issues.¹²⁷ As one of the NATO Centres of Excellences,¹²⁸ it is also a research and development Centre, which is composed of the NATO member countries and linked to the NATO Allied Command Transformation. The Centre has served as a useful interface between NATO military bodies, academia, the private sector and the EU. CCD COE is a body with large outreach capacity, including NATO nations' cooperation with the EU. The synergies of exchanging the best practices of different organizations have already started to materialize - ENISA and CCD COE have organized joint events on addressing cyberthreats.¹²⁹ The CCD COE Annual Cyber Conflict Conference has brought together leading European and North American cyber-experts since 2008,¹³⁰ and training events organized by the Centre have been very valuable for NATO countries' overall preparedness in cyberdefence issues.

3.5 Assessment

Internet governance is a catch-all term that only loosely encapsulates the sum total of very different cooperative and regulative frameworks that make up the Internet and cybersecurity. Overall, the informal self-started processes have often been more efficient than many top-down processes led by international organizations and governments. Trust-based information security experts' networks have shown their ability to mobilize needed expert knowledge and networks in most international cyber crises so far, and letting these groups do their work is absolutely critical for the future stability and resilience of the Internet. Governments and international organizations should consider maintaining the positive aspects of these informal networks when designing more formal cooperation and coordination mechanisms.

The UN shows the two different approaches that government can take on Internet governance: the top-level consultation and mediation approach, and the international organization approach. In the opinion of the authors, the first approach should be supported by the EU, while the latter approach should be resisted – at least in the short term. Firstly, a 'World Health Organization for Cyber' might quickly be taken over by special interests, and therefore would be a less-credible partner than directly-mandated national governments. Secondly, even large bureaucratic and mandated international organizations have shown that they are always challenged by the complexities of cybersecurity, even when their mandate is extensive.

NATO is a case in point for this. Few multilateral organizations have set such a high level of ambition, aiming to bring their scattered networks under central cyber-protection and surveillance, or are as well-equipped to deal with this task. However, NATO's efforts cannot go beyond its stated mandate to act as a collective defence and crisis management organization. NATO can encourage the Allies to build resilient national cybersystems, and deliver some support to civilian information infrastructure protection. But NATO is not mandated to enter the policy fields of civilian cybersecurity issues. Given the importance of civilian cybersecurity to overall cybersecurity, this is a critical omission. NATO can contribute only to the most strategic aspects of national cybersecurity, not cover the entire spectrum of different, mostly civilian, cybercapabilities.

However, NATO's efforts in setting up its cyberdefence position could potentially be complemented by the EU in leading the European nations' civilian cybersecurity activities (see next Chapter for EU

¹²⁷ See NATO, *NATO opens new centre of excellence on cyber defence*, 14 May 2008, <http://www.nato.int/docu/update/2008/05-may/e0514a.html>.

¹²⁸ See *ibid.*

¹²⁹ See CCD COE, *Joint Workshop on Countering Botnets*, 4 January 2011, <http://www.ccdcoe.org/221.html>.

¹³⁰ Cooperative Cyberdefence Centre of Excellence (CCD COE), <http://www.ccdcoe.org/>.

activities). This type of division of labor among 'widely-mandated' organizations is perhaps the only institutional approach that has any promise of success. A more promising approach for government engagement – and in particular for the EU – is to help its Members develop coherent positions for representation in the international frameworks, such as within ICANN. These types of representations occur on the basis of 'core values' and therefore are easier issues to address than issues that are almost always directly covered by national legislation.

4 CYBERSECURITY IN THE EUROPEAN UNION

4.1 The Nature of European Cybersecurity

The EU has approached the issue of cybersecurity in a fragmented manner, where parallel policies have sometimes been launched with different overlapping themes. Most of these initiatives have direct or indirect relevance to EU Members' preparedness to withstand serious cyberattacks, as they address the means and methods of cyberattacks, as well as the consequences of these attacks. However, the term 'cyberwarfare' is seldom, if ever, used, and there is very little unclassified material available that deals with the threats, consequences and responses to state-directed cyberattacks. This is relevant since, while most potential cyber national security threats can be dealt with by utilizing measures intended to combat crime and terrorism, some threats and types of attack will most likely never be utilized by a criminal or terrorist actor, as they require substantial resources to implement. These types of attack are likely to remain unique to state actors, and therefore to cyberwar.

Within the European Union there are two principal policy areas in cybersecurity that have particular relevance for cyberwarfare: First, there are measures intended to combat cyberattacks (including cybercrime/cyberterrorism)¹³¹ and second, measures intended to support Critical Infrastructure Protection (CIP), Critical Information Infrastructure Protection (CIIP) and Network and Information Security (NIS). There is substantial overlap between the two policy fields, and often the relevant Commission bodies consult with each other even when there is no clear requirement to do so. In comparison, the role of the Common Foreign and Security Policy (CFSP) is much less developed– in part due to its confidential and interdepartmental nature, but also due to the difficulties in approaching a subject perceived to be a matter often left to Member States.

4.2 Cyberattacks, Cybercrime and Cyberterrorism

The DG Justice and Home affairs have engaged in cybersecurity-relevant work at a substantial level detail - continuous work has been devoted to different legislative recommendations and policy documents. However, as a pre-Lisbon intergovernmental theme, it has suffered from chronic implementation setbacks. The good work of the European Commission and Council has often been hindered by the reluctance of Member States to harmonize national laws, to advance law enforcement capabilities and implement the Framework Decisions. On the other hand, many of these 'resisting' Member States have raised very legitimate concerns; such as regarding data retention and privacy issues that will need to be addressed by the Commission very soon. The failure to address data protection issues, in particular, threatens to undermine the entire legislative program in this area, and dealing with this issue should be an overriding priority.

4.2.1 Key Documents and Strategies

In 2005, the landmark **Council Framework Decision on Attacks against Information Systems**¹³² was adopted, which required all Member States to introduce legislation (by 2007) to deal with the principal types of cyberattacks, and, most significantly, which provided common definitions for such attacks. Member States thus agreed on definitions to what constituted criminal activity: 'Illegal access to

¹³¹ The EU does not make explicit reference to 'cyberterrorism', however the EU does imply that terrorists could potential execute serious cyberattacks.

¹³² Council Framework Decision on attacks against information systems, 2005/222/JHA, 24 February 2005, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193_en.htm.

information systems', 'Illegal system interference'¹³³ and 'Illegal data interference'.¹³⁴ The Decision also called for a common information exchange between Member States.

In the wake of the London and Madrid terror attacks, the **European Data Retention Directive (EUDRD)** was passed by the Council in 2007. This Directive requires all Member States to have legislation in place to ensure that the telecommunication companies and Internet Service Providers (ISPs) maintain records on user traffic (on connections, not however on content) for a maximum of two years. While the telecom companies largely do this already for billing purposes, many ISPs do not – making them effectively 'bullet-proof', i.e. making all activity conducted through them completely anonymous and cybercrime measures ineffective. The directive has been the subject of fierce criticism, mostly from data-protection groups suspicious of how the data generated will be used and protected from misuse. Implementation of the EUDRD has been slow, and by early 2011 not all Member States had implemented it.

In 2007, the European Commission issued the communication '**Towards a general policy on the fight against cyber crime**'¹³⁵ that sought to improve operational law enforcement cooperation, political cooperation and coordination among Member States. It also promoted political and legal cooperation with third countries as well as awareness -raising, training, research and a reinforced dialogue with industry for possible legislative action.

'Counter-radicalization', i.e. the ability to monitor and address violent ideological material, has long been a focus of the EU counter-terrorism strategies. In the 2005 **Counter-radicalization Strategy**¹³⁶ clear references were made to the importance of the Internet and the need to have better coordination among Member States in spotting websites of interest. This was developed in 2007 under the German Presidency in the '**Check the Web**' initiative¹³⁷; an information sharing portal maintained by Europol that provides a common registry of 'websites of interest'. The wide-scale success of this measure led to the project becoming fully institutionalized within Europol in February 2010.

In December 2009, the '**Stockholm Program**'¹³⁸ was accepted, which represented a significant step in the 'internal security' agenda of the European Union. Besides calling for a European Internal Security Strategy (see below), the program made a number of references to cybersecurity, including: the need to develop better and more resilient network information security measures, a 'better ability' to deal with cyberattacks, the importance of all Member States ratifying the Cybercrime Convention, and the importance of information exchange, both between governments as well as with the private sector.

Recently, DG Home Affairs has put cybercrime high on its agenda.¹³⁹ Towards the end of 2010, a **proposal was developed to adopt a new EU Directive on attacks against information systems**.¹⁴⁰

¹³³ Defined as 'the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data' (Ibid.).

¹³⁴ Defined as 'the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system' (Ibid.).

¹³⁵ See European Commission, *Towards a general policy on the fight against cyber crime*, COM (2007) 267 final, 22 May 2007, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.

¹³⁶ See Council of the European Union, *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*, 14781/1/05, 24 November 2005, <http://register.consilium.eu.int/pdf/en/05/st14/st14781-re01.en05.pdf>.

¹³⁷ See Council of the European Union, *Council Conclusions on cooperation to combat terrorist use of the Internet ('Check the Web')*, 8457/3/07, 29 May 2007, <http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf>.

¹³⁸ See Council of the European Union, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, 2 December 2009, <http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf>.

¹³⁹ See Vogl, Toby, 'Malmström seeks EU powers to tackle transnational crime', *EuropeanVoice.com*, 11 November 2010, <http://www.europeanvoice.com/article/imported/malmstrvm-seeks-eu-powers-to-tackle-transnational-crime/69374.aspx>.

The need for the new directive is based on a Commission review on the implementation of the Framework Decision on Information System Attacks¹⁴¹, which concluded that additional work needs to be done to harmonize the legal framework within the EU in the fight against cybercrime. This is particularly relevant against the background of the new sophisticated attack methods and technologies that are to be expected in the next years. The Directive will also assist Member States in advancing their law enforcement capabilities in the fight against cybercrime. The Directive has the potential to be one of the most far-reaching documents published by the EU, and if passed and implemented would significantly contribute to the resilience of European systems.

4.2.2 Key Programs and Institutions

Adopted in October 2010, the new **EU Internal Security Strategy** aims to raise the level of security for citizens and businesses in Cyberspace and attempts to deal with cybercrime issues head-on. Three specific proposals in the strategy include the establishment of an EU cybercrime Centre by 2013, the establishment of a network of Computer Emergency Response Teams (CERTS) in all EU institutions by 2012 (as well as the cooperation of these institutions with law enforcement), and the launching of a **European information sharing and alert system (EISAS)** by 2013. The key European initiatives are more in alignment with Network and Information Security than with DG HOME, although coordination between the two DGs does exist

In 2010 the Council agreed on a **Cybercrime Action Plan**¹⁴² that also called for Europol's **European Cybercrime Platform (ECCP)** to be strengthened, for better support for cross-border education of law enforcement agencies, and for better coordination internationally.¹⁴³ Europol has often featured as the focus of many of the new Council decision and recommendations, and the ECCP has recently been upgraded to a full-time initiative, with a number of subordinate initiatives. Member States have often seemed reluctant to invest more organizational powers in Europol. An important organizational initiative, the European Cyber Crime Centre, has been proposed and agreed upon a number of times since first being discussed around 2007. While an agreement was reached in June 2010 to set up the European Union Cybercrime Task Force as a precursor organization to the actual establishment of the Centre, the Centre itself is on an uncertain timeline.

4.3 Network and Information Security, CIIP and CIP

Until 2007, the EU's approach in CIIP was largely constrained to a sub-category of Information Society developments. Called Network and Information Security (NIS) in EU terminology, cybersecurity was regarded as a side-effect of the growing dependence on information and communication technology. After the 2007 Estonian attacks, DG INFSO raised cybersecurity on the agenda of EU ministers and launched the first EU CIIP policy. Progress in this area has not always seemed to be uniform. Partially, this is due to very different legislative environments under which national CIP policies operate, and which limit the scope for universally applicable approaches. Also, many Member States with advanced intelligence, cyber-surveillance and protection mechanisms have already included the CIP/CIIP issue in

¹⁴⁰ See European Commission, *Cybercrime*, September 2010, http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm#part_2.

¹⁴¹ Council Framework Decision 2005/222/JHA.

¹⁴² See Council of the European Union, *Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime*, 5957/2/10, 25 March 2010, <http://www.statewatch.org/news/2010/mar/eu-council-revised-cyber-crime-conclussions-5957-rev2-10.pdf>.

¹⁴³ See Council of the European Union, *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime*, 15569/08, 26 April 2010, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf.

their national security systems, and therefore only marginally support separate EU efforts in this field. This is especially to the detriment of less advanced Member States, who clearly need support to be able to develop their own programs.

Nonetheless, it should be pointed out that, unlike cybercrime, CIP/CIIP is a multi-dimensional field that impacts not only legislation but also different layers of regulation and governance. Globally, it is the norm for these processes to take many years to design and implement, and, from this perspective, the program advanced by the Commission is actually fairly ambitious. Most Member States are moving forward with major new EU initiatives in this area, such as supporting pan-European cyberexercises, adopting regulations for ISPs and enhancing information exchange. The greatest hurdle to the effective implementation of the Commissions' programs is probably the Commission itself – within DG INFSO, NIS is dealt with only at a relatively low level and by only a comparatively small staff.

4.3.1 Key Documents and Strategies

Two issues have defined European NIS: firstly, an economics-driven approach to stimulate and secure the development of an Information Society in Europe; secondly, the development of Critical Infrastructure Protection (CIP) as a security issue, originally closely linked to counter-terrorism.

Officially operating foremost under an 'economic development' mandate, NIS derived in part from the 2005-6 **i2010 initiative** and the European Commission **Strategy for a Secure Information Society** (2006). Most recently, in 2010, this was reinforced under the **Digital Agenda for Europe**,¹⁴⁴ which includes 14 actions aimed at improving Europe's capability to prevent, detect and respond to network and information security problems.

At least as important, however, has been the development of NIS in the area of CIP, an initiative that received much of its original impetus from counter-terrorism. In October 2004, the Commission published the **Communication 'Critical infrastructure protection in the fight against terrorism'**, calling for Member States to tighten their CIP policies to better prepare for the growing threat of terrorist attacks. Following this, a **Green Paper on a European Programme for Critical Infrastructure Protection**¹⁴⁵ was published in 2005 and further elaborated on in 2006 in the **Communication on a European Programme for Critical Infrastructure Protection (EPCIP)**. This communication notes that Europe's critical infrastructures¹⁴⁶ are highly connected and highly interdependent. It also recognizes how Europe's critical infrastructures are dependent on information technology, including the Internet and space-based radio-navigation and communication. The farsighted approach calls for a European response to the vulnerabilities that might occur as a result of the breakdown of essential services. This became the stated objective of EPCIP; to improve the protection of critical infrastructure in the EU. This objective is to be achieved by establishing: (1) a process for identifying and designating European critical infrastructure and measures to help protect them; (2) a number of facilitating measures¹⁴⁷,

¹⁴⁴ European Commission, *A Digital Agenda for Europe*, COM (2010) 245 final/2, 26 August 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>.

¹⁴⁵ European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection*, COM (2005) 576 final, 17 November 2005, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

¹⁴⁶ Those physical resources, services, and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

¹⁴⁷ Many of these paid for also by a counter-terrorist program, the five-year program 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks' (see website: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_en.htm).

¹⁴⁷ See European Commission, *Regulatory framework for electronic communications in the European Union*, December 2009, http://ec.europa.eu/information_society/policy/ecomms/doc/library/regframeforec_dec2009.pdf.

including the setting-up of a number of working groups, the commissioning of studies and reports (especially in the area of understanding interdependencies), and the establishment of the CIWIN emergency warning network; (3) a number of support measures for Member States; and finally (4) contingency and crisis management.

An EU directive on Critical Infrastructure Protection (2008/114/EC) was adopted in 2008 in order to identify and designate European Critical Infrastructure (ECI), and to create a common approach to improve its protection. The directive concentrates on the energy and transport sector, but lays a solid foundation of principles to enlarge the directive to other areas such as the ICT sector – a step intended for 2011-2012. The directive advocates general risk management guidelines (called ‘operator security plans’), security liaison officers and mandatory reporting, as well as the exchange of sensitive information among law enforcement authorities.

For the ICT sector, the revised **Telecommunications Framework Directive**¹⁴⁸, as well as a collection of amendments of former directives (2009/140/EC) represented a significant step in the harmonization of legislation, with a special focus on security. The Directive¹⁴⁹ represents a decisive step towards a Community-wide regulatory framework, which should be transposed into the legislation of all Member States. It specifies, among other things, the requirement for telecom providers to provide information of ‘incidents’ (including cyberattacks) to ENISA. Remarkably, prior to this, most European telecom providers were not even required to inform their own national regulatory bodies of such incidents. Furthermore, the Directive demands that Member States apply appropriate risk management measures to ensure a minimum level of services, and, if advised by ENISA, the Commission reserves the right to mandate that Members adopt technical measures based on international standards. This legislation is therefore an example of how the EU harmonization efforts can make very sizeable contributions to Member States’ cybersecurity.

In April 2009 DG INFSO tackled the issue of significant cyberattacks head-on with a Communication entitled **‘Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience’**.¹⁵⁰ As part of the Action Plan agreed upon at the Tallinn Ministerial Conference on Critical Information Infrastructure Protection, the Commission document announced a wide number of initiatives for this, including a number of working groups and information exchanges, a public-private partnership group¹⁵¹, the setting-up of a European Information Sharing and Alert and System (EISAS) and the organization of pan-European exercises to manage major Cyber-incidents (the first exercise was undertaken in November 2010). All Member States were called upon to have a fully-functioning CERT by the end of 2011, although the deadline has now been postponed to the end of 2012. It is also expected that in 2011 DG INFSO will present the results of a non-paper on **Principles and Guidelines for Internet Resilience and Stability**, and will play a decisive role in the meetings of the new **EU-US Working Group on Cybersecurity and Cybercrime**.

4.3.2 Key Programs and Institutions

The European Network and Information Security Agency (ENISA) is an EU agency supervised and financed by the European Commission DG INFSO. Originally set up in 2004 as an advisory body for the Member States and EU institutions in network and information security issues, ENISA has rapidly

¹⁴⁸ Chapter III (Security and integrity of networks), Article 13A.

¹⁵⁰ See European Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM (2009) 149 final, 30 March 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.

¹⁵¹ Known as the European Public Private Partnership for Resilience (EP3R).

established itself as an actor in the European cybersecurity community. Until 2009 the ENISA mandate only allowed it to function as a research body, although it was able to support a number of Member States in advising on operative matters (including how to set up a CERT). Member States agreed in 2009 to extend ENISA's mandate and resources; however, how exactly the role of ENISA will be expanded in the future is still a matter of deliberation. The new ENISA mandate¹⁵² is currently still under review, but in effect it formalizes many of the new roles that ENISA already assumed in 2010, such as coordinating Pan-European Exercises and facilitating discussions with the private sector. Further to that, the current proposal entails that ENISA would also set up a CERT for EU institutions and assume the associated responsibilities as defined in Article 13A of the revised Telecommunication Framework Directive.¹⁵³ Also, ENISA will be responsible for the European Information Sharing and Alert System (EISAS) which, potentially, could play a major role in improving European cybersecurity. It is expected that ENISA will play a stronger role in overseeing the security aspects of the EU telecommunications' sector. It will include the Internet Service Provider's mandatory incident reporting and the requirement for the Member States to apply appropriate risk management measures to ensure the level of services, and, if advised so by ENISA, the Commission may mandate Member States to adopt technical measures based on international standards for communication network security.

4.4 Common Foreign and Security Policy Measures

Cyber-initiatives within the European Common Foreign and Security Policy (CFSP) area have been far less developed compared to CIP or cybercrime areas. The Implementation Report of the European Security Strategy adopted in 2008 included cyberthreats as a new category of risks to European Security.¹⁵⁴ The report recommends additional work in this area, exploring a comprehensive EU approach, raising awareness and enhancing international co-operation. Within the CFSP, the European Defence Agency and the EU Military Council have been working on aspects of CNO since 2008.

Cybersecurity was identified as a key security issue in the report on the **implementation of the European Security Strategy (ESS)** submitted by SG/HR Javier Solana to the European Council in December 2008. In a subsequent 2009 workshop at the EUISS, a seminar was held to initiate a first discussion on the implications of the cybersecurity agenda for the EU as a whole and examine ramifications of cyber for the CFSP. The event was organized jointly with the General Secretariat of the Council of the EU and in cooperation with Estonia.¹⁵⁵ Around the same time, the EU military authorities initiated the first steps to **examine the feasibility of developing a common doctrine on CNO** (i.e. cyberwar). However, given the current relatively weak wider institutional framework of common EU command and control capabilities, it will be hard for the EU to build common cyberdefence capabilities, even within the relatively limited areas of 'operational CNO' that have already been explored within the **EU Battlegroup framework**.¹⁵⁶ Unless the EU militaries can establish a joint governance model for its

¹⁵² See European Commission, *Concerning the European Network and Information Security Agency (ENISA)*, COM (2010) 521 final, 30 September 2010, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282010%290521_/com_com%282010%290521_en.pdf.

¹⁵³ European Parliament and Council, *Directive*, 2009/140/EC, 25 November 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDE>.

¹⁵⁴ European Council, *Report on Implementation of the European Security Strategy. Providing Security in a Changing World*, S407/08, 11 December 2008, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf.

¹⁵⁵ See Institute for Security Studies, *Cybersecurity: what role for CFSP?*, 4 February 2009, [http://www.iss.europa.eu/nc/seminars/seminar/select_category/26/article/cyber-security-what-role-for-cfspbrussels-4-february-2009/?tx_ttnews\[ps\]=1230764400&tx_ttnews\[pl\]=31535999&tx_ttnews\[arc\]=1&cHash=206cccab0a](http://www.iss.europa.eu/nc/seminars/seminar/select_category/26/article/cyber-security-what-role-for-cfspbrussels-4-february-2009/?tx_ttnews[ps]=1230764400&tx_ttnews[pl]=31535999&tx_ttnews[arc]=1&cHash=206cccab0a).

¹⁵⁶ Simón, Luis, 'Command and Control? Planning for EU military operations', *EUISS Occasional Paper*, no. 81, January 2010, http://www.iss.europa.eu/uploads/media/Planning_for_EU_military_operations.pdf.

communications and information systems, progress in the area of cyberdefence will be very slow, and can at best achieve only a limited joint integrated capability. The **European Defence Agency** has carried out a few research projects on technology aspects related to cyberdefence, and is looking forward to cooperating with other international organizations in this field.¹⁵⁷

At present, there are very few organizations within the CFSP field that actively deal with cyber issues. Besides the relatively limited activities of the EDA and the **EU Military Committee (EUMC)** in this field, both the **Policy Unit** and **SITCEN** have made tentative moves to include cyber in their deliberations. However, in both cases, the operational capability to support the political deliberations of the Council, and the actions of the **High Representative and the European External Action Services** is very limited. There are also few appropriate structures for advising the **Council and/or COREPER II**¹⁵⁸ on cyber-issues or serious cyberattack. Serious cyberattack has until now been the domain of the **Council Security Committee (INFOSEC)** – a high-powered but secretive body that mostly concerns itself with Information Assurance issues.¹⁵⁹ Information Assurance is an absolutely critical area that directly impacts the existential security of the EU institutions; however INFOSEC does not have a CFSP mandate and therefore does not inform the CFSP -relevant bodies – even when there has been a probable state-sponsored cyberattack on EU institutions, something which has happened repeatedly in recent years at least. They do not directly inform **COREPER II**, which remains the responsibility of the **Political and Security Committee (PSC/COPS)**. The PSC has support for military crisis management (EUMS) and civilian crisis management (CIVCOM), but not for cyber-issues. The recently established **Committee on operational cooperation on internal security (COSI)** might be able to fulfill this role. However, if so, the narrowly defined ‘home affairs’ mandate of this Committee may be as inappropriate for responding to serious cyberattacks as an excessively military or CFSP mandate would be.

4.5 Assessment: EU Initiatives

If one classifies the overall cyberwar capability to reside in both ‘resilience’ and ‘deterrence’ issues (see Part 1.4.3), the EU is completely dedicated to a ‘resilience’ approach, and indeed has made significant progress in recent years. Of particular importance in the opinion of these authors have been efforts to harmonize criminal legislation, the build-up of European CIP and NIS measures, and efforts to fund research and development in Europe. While the authors of this study consider ‘resilience’ to be more important than ‘deterrence’, ‘deterrence’ measures (meaning, in effect, credible ways to respond diplomatically or militarily to a serious cyber-attack and thus prevent such attacks from occurring) certainly have a role to play in interstate cyber-conflict. For a ‘cyber-ed conflict’¹⁶⁰ scenario, i.e. a general state-to-state conflict where the actors are completely obvious and cyberattacks are only one of many different activities, the response mechanisms can remain the same as they would for any Article 42(7) TEU (‘mutual defence’) issue. However, for a ‘serious-cyberattack’ or ‘cyberwar’ issue without obvious attacker attribution the response mechanisms are much less clear. The applicability of both Article 42(7)

¹⁵⁷ See Hale, Julian, ‘New EDA Chief Exec Looking to Show Agency’s Added Value’, *DefenceNews*, 11. January 2011, <http://www.defencenews.com/story.php?i=5427857>.

¹⁵⁸ COREPER II (‘Committee of Permanent Representatives’) is one of the most senior decision making bodies within the EU. It consists of heads of mission (Ambassador Extraordinary and Plenipotentiary) and deals largely with political, financial and foreign policy issues.

¹⁵⁹ Information Assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. This includes processes and procedures for dealing with sensitive information, whereby various levels of protection (such as encryption, or shielding of electronic radiation) is applied to various levels of confidentiality. The EU recognizes four security classification levels.

¹⁶⁰ For more on ‘Cyber-ed’ conflict see Demchak, Chris, ‘Strategies for a Cyber-ed’, *World Atlantic Council*, 12 August 2010, <http://www.acus.org/publication/strategies-cybered-world>.

TEU and TFEU 222 ('mutual assistance in case of terror attack') is completely uncertain, and alternative responses must be considered.

Besides the very low level of information security within the EU institutions themselves, there are several 'gaping holes' in European cybersecurity as a whole, especially as far as 'real' cyberwar (i.e. serious state-executed cyber-attacks) are concerned. In particular, this is the lack of any program to secure the ICT supply chain from being compromised (e.g. through counterfeit Internet routers) or to protect against a nearly-undefeatable 'hardware-attack'.¹⁶¹ Countries such as the Russia, China, the US but also France and the UK have taken steps to protect against (or at least minimize) the threat of this most serious of all cyberattacks, but these programs are not available to the EU or most EU Member States. Without them, however, no real 'resilience' is possible.

A division of labor seems to be emerging that points to NATO to deal with its European countries' cyber-capabilities in clearly-defined military circumstances, whereas the EU is expected to progress with its already well-established policy fields in fighting cybercrime and developing CIIP/CIP. In essence, NATO could assume 'deterrence', while 'resilience' could be covered by the EU. This intended mirroring of the some aspects of the existing CFSP / NATO relationship¹⁶² has significant disadvantages as well as advantages. First and foremost, NATO itself does not use the term 'cyberdeterrence' in any of its deliberations, partially as deterrence is considered very difficult to achieve, but also because it requires clear common CNO policies which are as of yet still in development, even within NATO. Secondly the Non-NATO-Nations have to be operationally included in this strategy at an operational level, which automatically presents significant challenges. Thirdly, if the Union wishes to have a credible diplomatic role, it will have to include cyberattack issues in its general remit. In essence, the Council Secretariat and the European External Action Service must have the resources to be able to engage in the full-spectrum issue that is cyberpower – both on the diplomatic (attaché) level abroad and within the relevant CFSP consultation mechanisms at home. Finally, the actual ability of the EU to be able to function in any serious fashion is reliant in part on the ability to maintain the confidentiality, integrity and availability of its own communication resources. Information Assurance (i.e. 'resilience') measures are absolutely vital here, but the implementation of these measures within the EU institutions is at present woefully inadequate, considering the challenges they face. However, even at an optimal level of information assurance implantation cyberattacks will always have some measure of success, especially those conducted by state actors. To be able to have even a marginal hope of deterring these advanced serious cyberattacks the EU must be able to develop CFSP strategies to encounter what will be the most significant security challenge of the 21st century.

4.6 Key Cybersecurity Organizations in selected EU Member States.

The level of cyber-protection varies greatly across the EU Member States. As the subject of cybersecurity is still new to the public, very few open-source academic or policy papers exist on the preparedness of the EU Member States to cyber incidents, crises and attacks.¹⁶³ A short analysis below will serve as a snapshot of EU Members' preparedness in regard to cyberthreats.¹⁶⁴ Currently, EU Members could be

¹⁶¹ By 'hardware attacks' it is meant the physical manipulation (usually at point of manufacturing, or by intercepting the supply chain) of computer hardware devices such as routers and chipsets to allow an attacker direct access to a system. Most forms of Information Assurance are not able to deal with an attack at this level. They represent the most serious of all cyberattacks but, as they are difficult to execute, are rare and usually executed by state-actors.

¹⁶² For instance in the Berlin Plus Framework for sharing resources between the EU and NATO

¹⁶³ See ENISA, *Stock tacking report*, 19 September 2008, <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report>.

¹⁶⁴ This reflects the authors' personal opinion but is not by any means a comprehensive comparative study on an EU members' relative cyber preparedness.

divided to three or four groups as to their awareness and publicly known abilities to address the growing cyberthreat. The following summary is indicative only, and by no means complete.

4.6.1 Large Advanced Member States

The first group of countries includes larger EU Member States, such as (but not limited to) France, Germany and the UK. These countries have long since identified cybersecurity and the threat of cyberattack as a top-level national security issue, and have increasingly devoted significant governmental resources to the task. France and the UK have traditionally emphasized the national security aspects of cybersecurity, whereas Germany has taken a more civilian approach by supporting self-protection measures in the private sector.

France. Cybersecurity received central attention in the French White Paper on Defence and National Security 2008.¹⁶⁵ In 2009, the French Network and Information Security Agency (ANSSI) was formed by the General Secretariat for Defence and National Security.¹⁶⁶ The Agency acts as a national coordinating body for the information security of governmental networks, and hosts the national CERT, a 24-hour watch-centre, and is responsible for initiating and managing the national cybercrisis management plan, PIRANET¹⁶⁷ – considered by these authors to be one of the most advanced of such plans in Europe. ANSSI also plays a decisive role in French CIIP efforts, supporting the surveillance of sensitive networks, preventing attacks by advising on trusted products and services for public and economic actors, providing advice for governmental entities and operators of critical infrastructure, as well as communicating information security threats to the larger public.¹⁶⁸ The Agency also serves as an accreditation agency for certifying national networks, and issues the cryptology regulations for other governmental bodies. ANSSI issued a new strategy in 2011 that identified four key strategies and seven objectives, including connecting local cyberdefence to global cyberpower, the expansion of cryptographic measures especially with NATO and the French CIP program, the increase of cooperation with the non-state sector, particularly in the area of analysis, and a special emphasis on preventing identity theft as well as expanding the governmental legal remit in cyberspace.

Germany. In 2009, the Federal Office for Information Security (BSI) was re-designated as a national security authority, and acts as a central provider of ICT services to the government as well as providing support for information security to the wider public.¹⁶⁹ It works closely with the private sector and with providers of information technology. The BSI also acts as a certification and assessment authority for national government networks, and designs risk management tools and technological solutions for secure systems as well for public, open-source use. The BSI investigates security risks associated with the use of IT and develops preventive security measures. It publicly provides information on risks and threats related to the use of information technology and also analyses developments and trends in information technology.¹⁷⁰ The BSI is the main agency responsible for delivering the German CIIP strategy, UP-KRITIS, and maintains various information exchanges. It also maintains the federal government CERT-BUND, the ‘citizen’ CERT, and works with CERT-Verbund (a cooperation of various

¹⁶⁵ See Présidence de la République, *The French White Paper on defence and national security*, http://www.ambafrance-ca.org/IMG/pdf/Livre_blanco_Press_kit_english_version.pdf.

¹⁶⁶ See French Network and Information Security Agency (FNISA) / Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 2009-2011, http://www.ssi.gouv.fr/site_rubrique88.html.

¹⁶⁷ See ANSSI, *Exercice PIRANET 2010: l'État s'entraîne à faire face à une attaque de grande ampleur sur les systèmes d'information*, 25 June 2010, http://www.ssi.gouv.fr/site_article248.html.

¹⁶⁸ See ANSSI, *Core Missions*, http://www.ssi.gouv.fr/site_rubrique98.html.

¹⁶⁹ See BSI, *Taking advantage of opportunities – avoiding risks*, https://www.bsi.bund.de/cln_165/EN/TheBSI/AboutBSI/aboutbsi_node.html;jsessionid=44577CA316658235C4799B2E891309F6.

¹⁷⁰ See BSI, *Functions*, https://www.bsi.bund.de/cln_174/EN/TheBSI/Functions/functions_node.html.

private and public CERTs). In February 2011 a new national cybersecurity strategy was presented that, among other initiatives, announced the creation of a high-level National Cybersecurity Council to coordinate policy, to be supported by a National Cyber Response Centre, which would also assume a role in crisis management.

United Kingdom. The UK has traditionally had significant experience in dealing with comprehensive cyberdefence issues, and the newest national security documents have reinforced (and even expanded) this capability. In the 2010 UK National Security Strategy,¹⁷¹ cyberattacks were named as one of the four most serious threats to the UK. In the 2010 National Cybersecurity Strategy, the policy resources of the Cabinet Office and of GCHQ were expanded, and GBP 650 million earmarked to support a dedicated cybersecurity program. This aimed to expand what is already one of the most extensive (and, it must be said, publically known) cyberdefence capabilities in Europe. The Office of Cybersecurity and Information Assurance (OCSIA) coordinates together with the support of the Cybersecurity Operations Centre (CSOC) many of the national cybersecurity initiatives directly relevant to the government departments. Besides specialized organizations whose task is the defence of governmental systems, the UK is unique in maintaining a large organization dedicated to CIP, the Centre for the Protection of National Infrastructure (CPNI). The CPNI covers three specific threats to national infrastructure, including cyber, and also maintains the Public Private Partnerships and information exchanges with the private sector. Together with the Department of Business, Innovation and Skills (BIS) CPNI is also responsible for cyber crisis-management. The UK approach has also always acknowledged the need to work with other countries to develop relevant international law, and has postulated that the best way to deal with overall cyberattacks of whatever provenance was to increase the facilities needed to combat cybercrime.

4.6.2 Medium and Small Advanced Member States

This group has one principle in common – their smaller size and more limited resources compared to larger countries mean that cooperation (both nationally and internationally) is emphasized even more than among the larger states. The emphasis is thus on the mobilization of resources, although there are different ways to achieve this.

Estonia. Following the 2007 attacks, Estonia adopted a National Cybersecurity Strategy in 2008, which concentrates on applying an extensive system of security measures, increasing the level of competence and expertise in information security, and raising public awareness of cyberthreats in the whole society.¹⁷² The Estonian strategy has also set up a new advanced system for national critical information infrastructure protection and has an ambitious agenda in advocating international co-operation on cybersecurity. The National Cybersecurity Council serves as a high level decision-making and inter-departmental coordinating body. The Council oversees the implementation of the cybersecurity strategy and decides on most important cybersecurity issues at a strategic level. The Cybersecurity Council, which also includes critical private sector actors, is led by the Ministry of Economic Affairs and Communications and is subordinate to the National Security Council. The Civil Emergency Act adopted in 2009 determines the national response to cybercrises, led by the Ministry of Interior. The Act also redefines critical services to society, supports a national Critical Information Infrastructure Protection system and establishes the principles for public-private cooperation in national cybersecurity. The Estonian Informatics Centre (EIC), under the Ministry of Economic Affairs and Communications, acts as a

¹⁷¹ UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world*, March 2008, http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.

¹⁷² See Estonian Ministry of Defence, *Cyber Security Strategy 2008-2013*, http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

national cybersecurity agency and is responsible for governmental information security, for public-private partnership as well as for issuing standards for government entities in IT security. The National CERT is situated in the same centre and runs a nation-wide early warning system. EIC also manages the CIIP program in Estonia. A voluntary defence organization, the National Cyberdefence League, was recently announced as a further way to mobilize civilian resources in an emergency.

Netherlands: While the Netherlands has built a strong CIP program in recent years, the 2011 National Cybersecurity Strategy has outlined a number of steps specifically related to Cybersecurity. Building on strong pre-existing private-public partnerships, the Netherlands will emphasize 'cooperation' as its primary tool in cyberdefence. While the new principle organizations will be based within state structures, they will have strong non-state participation. In particular, (civilian) operational capabilities will be concentrated in the new National Cybersecurity Centre, while the political/policy coordination will be undertaken by the Cybersecurity Board. A specific national ICT Crisis Plan will be drawn up and preparations for this supported by an ICT Response Board. Information exchanges, both at the national and the international level, have been recognized as absolute priorities. To facilitate these exchanges, a number of counter-cybercrime initiatives and similar initiatives will be connected to the Centre, while CIP partners (key private sector operations) will also be allowed to connect to a new secure government communication facility, NCV. Overall, the Netherlands will seek to increase the 'individual resilience' of both companies and individuals to a number of threats, including espionage, and will invest in propagating information assurance measures.

Sweden. Based on its background of a strong 'total defence' system and civil emergency preparedness, Sweden has a strong tradition of information security. In 2009 several government agencies were merged into the Swedish Civil Contingency Agency, which also assumed the responsibility for national cybersecurity planning at the strategic level.¹⁷³ As an authority responsible for public safety, emergency management, and civil defence, the agency concentrates on cybersecurity from a national crisis management perspective. The operational cyber-tasks are allocated to the Swedish Postal Agency, where the national CERT (CERT-SE) is situated. Swedish law-enforcement authorities have far-reaching traffic analysis capabilities that are commensurate with the country's specific attitude to transparency and information. Sweden has carried out regular national crisis management exercises with cybersecurity components, and has issued a few national documents in raising cybersecurity awareness.

4.6.3 Other Member States

A third group of countries consists of European countries that have very recently started to reorganize their cybersystems, adopt new strategies and assign structures for a national cyber-effort. For instance, Latvia, Denmark, Poland, Austria (to name but a few) have recently started work on a dedicated national CIIP / cyberdefence strategy, are drafting new legislation, or have otherwise publicly announced efforts to deal with the wider issue. Most of these countries have not yet clearly defined what exact approach (i.e. civilian, military, or intelligence-led), what kind of emphasis (crisis management, CIIP, or intelligence), or even what kind of legal cooperation environment (completely voluntary or completely mandated) they will be aiming for. These countries can benefit greatly from the experience the more experienced Member States, and should be assisted in attempts to get the necessary 'lessons learned' to help develop their own capabilities.

Finally there is also a fourth (smaller) group of countries that has not publicly declared new initiatives, strategies or organizations. It does not mean that these countries are not prepared for cyberattacks, but with the limited information available about their efforts in cybersecurity, there is probably a need for

¹⁷³ See Swedish Civil Contingency Agency, <http://www.sweunb.se/swedish-rescue-services-agency.aspx>.

raising awareness and giving more political attention to the issue of cybersecurity. Further, these countries do not actively engage in the relevant EU policy and working groups, either due to the intelligence-specific nature of their organization, or (more likely) a definite lack of the capability to deal with the issue in the first place. As these countries might not even be in a position to interact with more advanced States (due to a fundamental lack of resources of every kind), it is up to the Commission to directly provide support to these States in order to at least help them develop the most basic cyberdefence capabilities.

4.6.4 Overall Member States Assessment

Each country needs a coordinated and nationally-organized approach to cybersecurity, certain elements what should be in place in all national systems. The first step is to start reviewing strategic documents and advancing or establishing a national system for Critical Information Infrastructure Protection and the Public-Private Partnerships and information exchanges that usually are a mandatory feature. Each nation also needs operational and policy capabilities to enhance the situational awareness of cyberrisks. Countries need a national CERT and a standardization or advisory body for IT security which can serve as a major competence centre for public and private organizations in information assurance, and which has the potential to either work with or become the designated national security authority for participating in international cooperation. Besides these operational components, there must also be relevant policy bodies that are able to interface directly with political leadership at the highest levels. Considering the fluid nature of cyberthreats and the difficulties in attribution, the most efficient national cyberresponse systems are those that can mobilize both public and private sector resources in times of crises. As virtually all conflicts in the future will at least have some cyber component, both national civil emergency response procedures and national defence mechanisms must include the cyber as a 'mainstream' topic, and not an individual feature, such as 'airpower'. Finally, cybersecurity needs a continuous investment in skills and education, both for government agencies and the public at large, and this should be the central focus in every national strategy-level document.

5 ASSESSMENT AND RECOMMENDATIONS – 23 POINTS

Serious cyberattacks are one of the most significant security challenges of the 21st Century. A consistent issue across Europe, both among EU institutions and within most Member States, is a chronic underfunding of most cybersecurity-related functions in government. Archaic budget structures and the cross-departmental (multi-jurisdictional) challenge of cybersecurity have meant that even modest budgets can have difficulty being approved. Within the EU institutions, cybersecurity has largely been approached in an ad hoc manner, with a number of different initiatives being executed by a number of different bodies, with only marginal coordination. While this has contributed to overall 'resilience' much needs to be done, and there is virtually no CFSP component in what is surely one of the most global of themes.

5.1 Assessment

1. Currently, the **overall level of self-protection of the EU institutions from cyberattack is relatively low**. The EU does not have a single overall Computer Emergency Response Team (CERT) to help them protect their networks. While such a CERT is planned at ENISA for June 2011, the actual extent of its mandate and capability is unclear at this time. This is especially problematic given the wide range of cyberattacks that almost all EU institutions have been subject to – a situation that doubtlessly will continue to worsen in the future. Without a fully-functioning CERT with adequate resources as well as functioning Information Assurance measures, no basic work on cybersecurity can be successful. Overall, while the official Information Assurance (IA)¹⁷⁴ requirements within the EU are high, the actual implementation of these measures is uneven. Anecdotal information as well as the personal experience of the authors has shown that the implementation of many IA measures in all relevant institutions can best be described as 'patchy'. IA measures within EU institutions certainly appear to be much less stringently enforced than in many Member governments. At the same time, the EU institutions' networks have repeatedly been penetrated successfully in CNE attacks. Many of these attacks could have been prevented by better Information Assurance measures, or even better implementation of already existing regulations. Although the Council and Council Secretariat have regularly exchanged information regarding severe cyberattacks, much of this information has not been shared with European officials actually responsible for many of the relevant policy areas, or with MEPs in the relevant committees. One reason for this is the lack of high-level security accreditation for many EU officials and MEPs – most of the information is exchanged at SECRET UE or higher levels, and many officials and MEPs do not have these clearances or indeed any clearance at all. Hence, many of the officials and MEPs who actively work in the wider area of cybersecurity do not have even the most basic information on past cyberattacks against the EU.
2. While there are **many disparate elements that together make a 'European cybersecurity policy', there is no actual centre** that can tie together the disparate elements such as cybercrime, NIS, CIP, Internet governance, intelligence exchange, etc. into a reasonable whole. There is no 'European view' on how to react to state-sponsored cyberattacks, and many of the relevant EU-institutions do not have the policy resources to be able to adequately examine the

¹⁷⁴ Information Assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. This includes processes and procedures for dealing with sensitive information, whereby various levels of protection (such as encryption, or shielding of electronic radiation) is applied to various levels of confidentiality. The EU recognizes four security classification levels.

issue. The EU is developing a military CNO policy within the relevant structures of the Council Secretariat, but progress has been slow. The EU is not represented in many international discussions on 'cyberwarfare-type' topics, although these topics have an obvious relevance to CFSP. The application of current international laws on armed conflict, the deployment and use of cyberweapons, concepts such as 'cyberneutrality' (for nations as well as key Internet infrastructures) and nation-state responsibility to prevent their non-state actors from attacking foreign nations are major international issues being debated, often without any EU representation. European cybersecurity as a whole often depends on the cybersecurity of non-EU nations (including developing nations), but there is no recognition that supporting cybersecurity measures (while being cognisant of the dangers to fundamental rights if these measures are misused) needs to be part of both CFSP and development cooperation.

3. Although the Commission has become increasingly active within ICANN, the level of operational **engagement in Internet governance continues to remain relatively low**. Awareness of the security implications of Internet governance has recently increased, leading to a revision of some EU positions, but in general the subject is not understood to also be a very important security issue. The EU as a whole has a strong role in many of the Internet governance bodies, but its positions are not always well coordinated or represented.
4. Cybersecurity is a comprehensive issue with clear relevance to the CFSP, but there is seldom any mentioning of international cybersecurity as a component of CFSP, and **global cybersecurity-issues have currently virtually no role whatsoever within the CFSP**. There is certainly **no concept of projecting 'hard' or 'soft' power via an integrated approach to cyberpower, and therefore for helping to define international cybersecurity around the core values of the Union**. Currently, there is no clear alignment of cyberwarfare-relevant issues, especially as the Lisbon treaty is still in the process of implementation. On a working-group level, a joint DG Home and RELEX working group is responsible for reviewing foreign policy matters that are related to internal security issues – however, it is unclear to what extent state-sponsored cyberattacks have been dealt with within this group. Within the Council, the Council Security Committee (CSC or INFOSEC) is the only body that has been privy to information pertaining to serious cyberattacks, supported by the Commission Security Directorate and SITCEN. It is not clear to what extent this information has been shared outside of the INFOSEC membership, and it does not seem that the Political Security Committee (PSC) receives any information. The PSC prepares CFSP matters for COREPER II, and, on serious cyberattack issues, is presently advised by the European Union Military Committee (EUMC) and/or SITCEN. Recent reforms have meant that the PSC will probably work more closely together with the new Committee on operational cooperation on internal security (COSI). It is currently unclear if COSI, PSC, or INFOSEC will advise COREPER II on cyber-issues in the future.
5. Overall, a number of EU initiatives have played an **important role in helping protect Europe from serious cyberattacks, especially by supporting 'resilience'**. Particular areas of strength are the EU research programs supported by the Commission. The contribution of the FP7 research program (as well as more specialized calls by various DGs) to European cybersecurity as a whole has been very significant and, as the result of past projects are being increasingly shared, will only rise in importance. While there is no objective data at this time as to the economic impact of these research programs, anecdotal information suggests that these research programs have considerably benefited Small Medium-Enterprise ICT companies, and thus also help support the European 'Digital Agenda'. The EPCIP program is a very important tool for raising awareness of these issues within the European governments and the private sector. Equally important are a

- number of measures intended to help increase the stability and resilience of European networks against serious cyberattacks, and to help harmonize Member State legislation regarding Network and Information Security and cybercrime.
6. For the majority of the Member States, the **European Commission has taken a leadership position on these issues, and has thus been instrumental in helping to drive the issue at a Member State level as well.** This importance of the leadership role of the EC should not be understated: while some (mostly larger) Member States would proceed with cybersecurity issues on their own, a significant number of Member States are very much reliant on EU initiatives in this area to be able to adopt the issue at home. Therefore, despite complaints by the officials of various Member States about the ambitious schedule and required workload of a number of Commission (and in particular NIS) initiatives, very few Member State officials would probably actively seek to constrain these initiatives, as they play a decisive role in driving the issue within national political agendas. The most serious impediment to many of the EU's own programs arises due to the lack of attention paid to these initiatives by senior officials. For instance, most of DG INFSO's activities in this area are addressed by a single sub-unit. Consequently, the lack of seniority on the part of the EC officials in the relevant policy and working groups often means that the initiatives do not get sufficiently high-level attention within the Member States' governments. Also, the lack of senior Commission engagement makes interaction with non-EU partners (in particular with the United States) inconclusive and at times confusing.
 7. Present **EU cybersecurity initiatives have also not sufficiently addressed the non-state sector.** Addressing the non-state sector (meaning both civil society and the private sector) is absolutely crucial in any attempt to increase 'resilience', develop a 'European' answer to serious cyberattacks, or even to help define a specific cyberpower policy. The importance of the civil society cannot be overemphasized; it ranges from volunteer technical actors in creating open-source software and patching and fixing existing protocols, to the research functions of civil society groups publicly investigating cyberattacks, to fundamental rights advocacy groups. The EU has always been relatively open to the role of civil society and therefore should not find it too challenging to increase consultation with this group. A bigger challenge for EU institutions will be expanding direct contact with the private sector. While this is already underway in a limited form (for instance the European Public Private Partnership for Resilience) it probably needs to be greatly expanded – many of the private sector initiatives in the Member States in this area (Public Private Partnerships and Information Exchanges) are often limited to 'national' companies and do not adequately reflect the cross-border nature of the private sector in Europe today. This is particularly acute in the area of information exchange (the sharing of cyberattack information among different organizations), which would benefit from a European industrial-sectoral approach.
 8. Many **EU Member States (as well as all EU institutions) are significantly vulnerable to 'hardware attacks' on their ICT systems.** There is no EU-wide program for securing a critical ICT supply chain similar to the United States 'trusted foundry' program, which seeks to guarantee that highly critical hardware components cannot be manipulated. Similar programs are active within Russia and China, and to some extent are even more wide-spread than in those active in the US. While the US program is not without its critics, the current need of the EU and most EU Member States to depend on commercial off-the-shelf components even for its most critical information systems puts it at direct risk to serious cyberattacks.
 9. **A major difference between cybercrime and cyberwarfare is the applicability of criminal legislation versus national security legislation.** This is especially acute as there are scenarios in

which one Member State is subject to a critical cyberattack via another ('third party' or 'transit') Member State. To support the Member State under attack, the 'transit' Member State might have to take measures that can result in collateral damage to its own civilian systems - for instance, by disrupting the availability of crucial ITC services to its own private companies. However, under criminal legislation, most Member States might find it legally difficult to inflict this 'collateral damage' on its own citizens. Under national security legislation, however, measures like these are more likely to be legally possible

Two principle elements of European legislation currently exist to deal with serious cyberattacks. Article 42(7) TEU ('mutual defence clause') clearly requires Member States to assist each other in case of an 'armed aggression occurring on its territory'. However, it is not yet completely clear that the Article 42(7) would apply even in case of a debilitating act of cyberwarfare occurring against a Member State – that is, even if the act can definitely be attributed to another country. Article 222 TFEU ('mutual assistance clause') offers another substantial instrument for cooperation, stating that *The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or natural or manmade disaster...shall mobilize all instruments at its disposal.* Thus, within the context of referring to a 'cyberterror' rather than a 'cyberwarfare' attack, similar resources can be mobilized by Member States. Article 222 TFEU also calls upon the Council to *'regularly assess the threats facing the Union, in order to enable the Union and the Member States to take effective action'*, which implies that the Council can be called upon to provide threat assessment encompassing serious attacks against Critical Infrastructures as well¹⁷⁵.

One considerable difficulty is the implicit definition of 'terrorism' as always being conducted by an organization, itself defined by a hierarchy. It is doubtful that most current serious cyberattacks could be classified in this manner, since they are carried out by 'unknown individuals'. Thus a redefinition of the term 'terrorism' might be necessary, but it must avoid the possibility of misuse to suppress or undermine fundamental rights.

10. **European integration is not only achieved via EU institutions, but also by a number of bilateral initiatives and cooperative agreements between EU Member States.** These initiatives can contribute greatly to European cybersecurity. Foremost among them is the European Government CERT Group (EGCG). The group sets its own membership standards (only a few Member States currently meet the requirements) and is not subordinate to any EU institution. This independence is strength rather than a weakness, and EU institutions should resist the temptation to try to regulate successful independent ventures. Cooperation between such groups and EU institutions, on the other hand, is a different matter, and should be encouraged, where viable.

5.2 Recommendations

While the EU can build on a number of successful initiatives strengthening the general 'resilience' of Europe against serious cyberattacks, the level of self-protection in EU institutions, in particular against

¹⁷⁵ A recent Swedish Analysis on TFEU 222 concluded that 'state-sponsored Cyber-attacks against strategic infrastructure network in MS' would be covered by TFEU 222 (see Myrdal, Sara and Rhinard, Mark, *The European Union's Solidarity Clause. An Analysis of Article 222 of the Treaty on the Functioning of the European Union*, Swedish Institute of International Affairs, 2010, <http://www.ui.se/upl/files/44241.pdf>). EU officials consulted on this issue were however less clear that 222 applied, unless a 'specific terror group' could be identified.

sophisticated (state-directed) cyberattacks, is low, and compromises the basic functioning of the EU institutions. Similarly, there are virtually no foreign-policy structures in place to help promote any form of 'deterrence' against such attacks in the future, or even help promote European core values within international cybersecurity.

1. All EU Institutions should **urgently increase the level of their Information Assurance (IA) measures**. This in particular includes adequate support for the planned EU-CERT, as well as increased implementation of IA measures to safeguard the confidentiality and integrity of EU communication and information systems. While common measures are being developed, EU institutions should consider expanding their independent IA resources until common resources can be deployed. This particularly applies to the High Representative, the European External Action Service as well as the Council Secretariat bodies such as SITCEN.
2. All EU institutions should **consider expanding the number of officials and MEPs with security accreditation up to and including SECRET UE**. This is to facilitate information exchange and to enable necessary briefings on past cyberthreats. Similarly, the Commission and Council should consider enabling the wider dissemination of information on cyberattacks at lower levels of classification (below SECRET UE) so that more officials and MEPs have at least a basic appreciation of the scale of the current challenge. Recent steps in this direction, particularly within the European Parliament (accreditation of MEPs) should be continued.
3. The Council should **clarify the roles of the PSC, COSI and the CSC (INFOSEC) as far as serious cyberattacks are concerned**. In particular, the issue how COREPER II is briefed needs to urgently be addressed. Potentially, a separate consulting body on cybersecurity issues could be established to support the PSC.
4. All EU institutions should acknowledge the **importance of Information Exchanges and Public-Private Partnerships (PPP) in improving cybersecurity**. The Commission, which has recently inaugurated a PPP of its own, should strive to support Members seeking to build up PPPs of their own, but need support on how to proceed. Equally, the Commission should examine the feasibility of providing frameworks to enable national PPPs to cooperate with each other in a European sectoral (e.g. 'Energy, Financial Services') context.
5. The European Parliament should consider **holding hearings on 'Serious cyberattacks against the EU institutions and EU Member States'**. It is a matter of urgency that the Parliament be appraised of the seriousness of the present situation, in particular as it applies to CNE (cyberespionage) as an ongoing problem. Further, the potential for cyberattacks which could cause serious disruption to European Critical Infrastructure needs to be considered and examined in depth.
6. The European Parliament **should call for the appointment of a 'Cybersecurity Coordinator'** to help integrate the diverse initiatives, programs and activities across the EU institutions.
7. The European Parliament should evaluate, together with the Council and the Commission, the feasibility of **funding a 'Structural Cybersecurity Funding Instrument'** that can assist all Member States in implementing the various Decisions and Directives as well as raising their overall organizational and technological cybersecurity level. For countries that have 'significant' resource challenges, additional funding could be made available to directly subsidize operational activity within cybersecurity.
8. The European Parliament should reinforce previous calls of the Council and the Commission for Member States to universally ratify **the Council of Europe Convention on Cybercrime**. Most EU

- Member States are already signatories to the convention, but all Members should seek to ratify and implement the convention as soon as possible. All follow-up attempts that build on the Convention should be supported.
9. The European Parliament should urge the Council to draft relevant proposals to **incorporate issues of cybersecurity within the mandate of the CFSP in a 'CFSP Cyber Agenda'**. This agenda should include
 - a. An appreciation of the **importance of Internet governance** as a security topic, and the need for common positions on key issues,
 - b. The planned participation in **international discussions on developing the norms** of responsible state behavior in cyberspace, including addressing *jus in bellum* and *jus ad bellum* issues,
 - c. The inclusion of cybersecurity **as a subject area within the European External Action Service**, either as part of the existing attaché structure or with its own dedicated attaché,
 - d. The need to **evaluate a Whole of the Union response to serious cyberattacks**, as well as assessing which types of instruments (diplomatic, information, military, economic) could be brought to bear,
 - e. The **better coordination of existing Commission initiatives** on cybercrime, Network and Information Security and CIP/CIIP,
 - f. Support for the work of the **EUMC in drafting common policy frameworks**, especially on a joint CNO doctrine,
 - g. Resources for the Council Secretariat to adequately **exchange and process information relevant to serious cyberattacks** (in particular within the EEAS, SITCEN and the Policy Unit),
 - h. New **initiatives within the European Defence Agency** to help support the cyberdefence capabilities of Member States,
 - i. A review of **which International Organizations are most relevant for both policy and operational cooperation mechanisms**, and where the EU should seek to expand cooperation, if appropriate. In particular, the Council of Europe, the OSCE, the UN Family and NATO should be considered important partners. Closer cooperation with informal international forums on cybersecurity (e.g. Meridian, FIRST) should also be considered.
 10. The European Parliament should request the Commission to **acknowledge the direct relevance of cybersecurity in developing countries to the cybersecurity of the EU as a whole**. In particular, 'cybersecurity assistance programs' could be evaluated as a potential extension of the current instruments for development cooperation.
 11. The European Parliament should urge the Council to **examine the prospect of creating a 'European Trusted Foundry'** or similar program to protect its ICT supply chain (in particular microchips) from hostile manipulation.
 12. The EU Parliament should urge the Council and the Commission **to expand its engagement with non-Member States** (in particular Russia, China, Brazil, India and the United States). Where closer mutual understanding has already been achieved (for instance, recently with the US), the EU should consider expanding the number of joint activities.

13. The European Parliament and the Commission should examine **potential community funding instruments to directly assist the private sector in building cybersecurity**, given the extensive damage caused by cybercrime to European businesses. The individual Member State programs, where they exist, should not be duplicated, but complemented.

5.3 Concluding

The EU has made important contributions to helping to develop the 'resilience' of EU Member States to serious cyber-attack. However, these measures need better coordination, should be expanded upon, and most importantly need to be understood as not only an 'internal' or 'economic' issue, but also as a Common Foreign and Security Policy issue. More than perhaps any other subject in modern day government, the challenge of 'cyber' transcends traditional divisions such as 'internal' vs. 'external' affairs' or 'security' vs. 'economic' domains, standard government departmental organizations, or even classifications such as 'state' and 'non-state'. Ambiguity is the defining reality of this new domain, and only the actors that are able to work with this ambiguity will be able to exercise any form of 'hard' or 'soft' cyberpower in the future.

APPENDIX I: TYPES OF CYBERATTACKS – A PRIMER

There is a wide range of cyberattacks: they can be used for purposes of crime, terrorism or warfare. In general, these attacks can be segmented into ‘technical attacks’ and ‘social attacks’. Usually, the two operate together to achieve an objective – such as getting access to a computer network. Ultimately, however, most cyberattacks are focused on influencing human behaviour in one form or the other. Therefore the most advanced and dangerous attacks are not necessarily those with the highest level of technical proficiency, but those that have the most significant impact. Gaining access to the most closed or secured systems, for instance, is best accomplished through tricking individuals to reveal their passwords, rather than brute attacks on the system itself.

‘**Hacking**’ is often used as a catch-all term to refer to a wide range of attacks. When used within a purely technical context, hacking usually refers to the process of exploiting holes (errors) in software to enable an attacker to gain access to a system. Using, for instance, a SQL¹⁷⁶ exploitation attack on an unprotected website it is possible to gain access to databases, such as those with personal information and user credentials.¹⁷⁷ Once the hackers have these credentials they can subsequently attack other networks that are not vulnerable to SQL attacks, simply by using the captured user credentials and passwords. They can also modify and change the website, either ‘defacing’ it with propaganda material or similar, or even use the website to launch a ‘drive by attack’ that can download malicious programs – ‘malware’ – on a user. **Malware**¹⁷⁸ includes a wide range of attacks including **Trojans** (disguised programs which execute hostile action such as stealing information or providing access), **viruses** (which replicate and seek to contaminate other programs), **worms** (similar to a virus, only that they seek to expand to other networks as well) and others. The amount of malware in circulation has risen exponentially in recent years, from an average 5000 new malware programs in 2007 to over 63,000 new malware threats in 2010.¹⁷⁹ While eventually 99% of all malware is blocked by daily-updating anti-virus software, this still leaves many that are not discovered before an attack is executed. More complicated attacks often combine aspects of different malwares, and are known as **blended** or **hybrid attacks**. Some of these attacks are also called **Advanced Persistent Threats (APT)** and specialize in data-extraction (CNE, or cyberespionage). Not being directly connected to the Internet provides only limited protection – advanced worms (such as Stuxnet) are designed to travel from one closed system to the other (for instance via USB thumb drives) before becoming active. Highly malevolent programs called ‘**logic bombs**’ can be transported by worms or planted directly on systems. These software packages are relatively small, and, as they do not need to communicate, extremely difficult to locate. Once triggered, they can be massively destructive, as a court case in the United States in 2008 illustrated: a logic bomb planted in the US mortgage giant Freddy Mae by a disgruntled employee would have wiped out all 4,000 servers if it had been allowed to detonate.¹⁸⁰

An increasingly visible form of attack is the **Distributed Denial of Service (DDoS)** attack, in which a number of infected computers (zombies or bots) are tied together into a **botnet**, and are remotely controlled via command & control computer and are used to attack websites, ‘flooding’ them with

¹⁷⁶ A database-focused computer language often used in conjunction with websites.

¹⁷⁷ Harper, Mitchell, ‘SQL Injection Attacks – Are You Safe?’, *sitepoint*, 17 June 2002, <http://articles.sitepoint.com/article/sql-injection-attacks-safe>.

¹⁷⁸ Beal, Vangie, ‘The Difference Between a Computer Virus, Worm and Trojan Horse’, *Webopedia*, 29 June 2010, <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.

¹⁷⁹ See Panda Security, *One-Third of All Malware was Created in the First 10 Months of 2010*, 24 November 2010, <http://press.pandasecurity.com/usa/news/one-third-of-all-malware-was-created-in-the-first-10-months-of-2010/>.

¹⁸⁰ See Claburn, Thomas, ‘Fannie Mae Contractor Indicted for Logic Bomb’, *InformationWeek*, 29 January 2009, <http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=212903521>.

requests and either closing them down completely, or making them vulnerable to hack attacks. Botnets are primarily used for cybercrime purposes – spam, theft of credentials, and similar, and can generate substantial profits for their operators.¹⁸¹ Botnets can be huge – in March 2010 the botnet ‘Mariposa’ controlled over 13 million computers worldwide. It was mostly used to steal credentials and send spam, but before being shut down its operators executed a DDoS attack on the anti-virus company working to defeat it.¹⁸² DDoS attacks have been used against a wide range of targets, including in defence of Wikileaks in 2010, against the US and South Korea in 2009,¹⁸³ and Estonia in 2007.¹⁸⁴ It is also theoretically possible for a DDoS attack to be directed against the root infrastructure of the Internet itself, in the most extreme case even leading to the temporary collapse of much of the Internet.¹⁸⁵ Attacks on the Internet infrastructure itself have already occurred a number of times, and do not necessarily lead to the collapse of the Internet. There have been at least four clear instances where (accidentally or intentionally) the Domain Name System (DNS) of the Internet was attacked. In an incident in April 2010, a ‘rogue’ Chinese name server managed to temporarily hijack up to 10% of the World Wide Web, routing it through China and in effect subjecting a good portion of the world’s information flow to the ‘Great Firewall’ of China – the automated Chinese web censorship regime.¹⁸⁶

Social attacks have always been a vital part of gaining access to closed systems. On the whole, they descend from an attack-type known as ‘**social engineering**’, in which an attacker assumes the guise of a legitimate user and, for instance in a phone call or in an email, tricks the victim to reveal password credentials, identification numbers, or even just personal information that can be used to guess passwords from. More recently, **phishing** scams are emails that purport to be legitimate (such as from a bank) and which seeks to direct a user to a fake website where they enter their credentials, or which downloads malware (such as a Trojan) onto their system. The most advanced forms, **Spear Phishing** attacks, target only a few highly placed individuals and are very sophisticated – impersonating existing persons from acknowledged institutions. Governments have often been the target of these types of attack, for instance by Chinese attackers.¹⁸⁷ Considerable amount of reconnaissance, increasingly conducted over social networks such as Facebook, needs to be conducted to be able execute these attacks.

Much of what is called ‘Critical Infrastructure’ depends on specialised IT systems mostly referred to as **SCADA** (Supervisory Control and Data Acquisition). SCADA systems can control everything from a building’s air-conditioning to heavy machinery, and are ubiquitous in modern life. The vulnerability of SCADA systems to cyberattack has long been appreciated, although action on addressing these vulnerabilities has been comparatively slow. A number of SCADA attacks on critical infrastructure have

¹⁸¹ SPAMfighter News, *Botnets Help Cyber Criminals Earn Huge Revenues, says Kaspersky*, 8 August 2009, <http://www.spamfighter.com/News-12870-Botnets-Help-Cyber-Criminals-Earn-Huge-Revenues-says-Kaspersky.htm>.

¹⁸² See McMillan, Robert, ‘Spanish Police shut down ‘world’s largest’ botnet’, *Techworld*, 3 March 2010, <http://news.techworld.com/security/3214049/spanish-police-shut-down-worlds-largest-botnet/>.

¹⁸³ See Kirk, Jeremy, Probe into US, South Korea cyberattacks stretches around the globe, *ComputerworldUK*, 15 July 2009, <http://www.computerworlduk.com/news/security/15724/probe-into-us-south-korea-cyberattacks-stretches-around-the-globe/>.

¹⁸⁴ Espiner, Tom, ‘How Estonia’s Attacks Shook the World’, *ZDNet*, 2 May 2008, <http://www.zdnet.com.au/insight/security/soa/How-Estonia-s-attacks-shook-the-world/0,139023764,339288625-3,00.htm>.

¹⁸⁵ See Vaughan-Nichols, Steven J., ‘How to crash the internet’, *ZDNet*, 13 February 2011, <http://www.zdnet.com/blog/networking/how-to-crash-the-internet/680>.

¹⁸⁶ See, for instance, BGPmon, *Chinese ISP hijacks the internet*, 8 April 2010, <http://bgpmon.net/blog/?p=282>.

¹⁸⁷ See Glanz, James and Markoff, John, ‘Vast Hacking by a China Fearful of the Web’, *New York Times*, 4 December 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=2.

been reported, in particular within the electricity generation sector.¹⁸⁸ As these attacks are less interesting to cybercriminals and can have severe public consequences, they are particularly relevant for cyberwarfare scenarios.

¹⁸⁸ For a good overview see, for instance, Averill, Bruce and Luijff, Eric A.M, 'Canvassing the Cybersecurity Landscape: Why Energy Companies Need to Pay Attention', *Journal of Energy Security*, 18 May 2010, http://www.ensec.org/index.php?option=com_content&view=article&id=243:canvassing-the-cyber-security-landscapewhy-energy-companies-need-to-pay-attention&catid=106:energysecuritycontent0510&Itemid=361.

APPENDIX II: LEVELS OF CYBERATTACKS – EXAMPLES

Level 1: Cyberespionage and Nuisance Attacks

According to the AF-SAB model, Level 1 cyberwarfare also includes ‘cyberespionage’ (CNE) as well lower-level disruptions of service. CNE is certainly a significant threat – some observers have even indicated that it is the most serious threat of all – but it is far from new. One of the earliest cybercampaigns, known as **Moonlight Maze**, occurred in 1998–2000. A large amount of confidential information was stolen from the US Department of Defence, Department of Energy, NASA, and a number of private institutions. According to some reports, the attacks were traced back to a server linked to the Russian Academy of Sciences in Moscow, and were attributed both to Russian cybercrime and the Russian Federal Security Services (FSB).¹⁸⁹ An even more sophisticated and massive cyberespionage campaign code-named **Titan Rain** began in 2003, and led to the wide-scale breach of classified US government and military systems,¹⁹⁰ with the loss of 10-20 terabytes of information.¹⁹¹ These attacks were traced to Guangdong province, China, and the same group of attackers was still active at least in 2007. Here, as well, non-state hackers and the state security services are presumed to be working in cooperation with each other.¹⁹² There have been a wide range of similar attacks on government systems, including on probably every single EU Member State and the EU institutions themselves. Details on the vast majority of these attacks, and the damage they may have caused and who the culprits might have been is classified, and has largely been unreported in the media. The widely-publicised 2010 Chinese CNE attacks on **Google (‘Aurora’)** illustrated that, even after a decade of exponentially increasing cyberespionage attacks, a number of factors have remained remarkably constant. Firstly, many of the attacks are executed by non-state actors, who however are working either with the consent or even the active cooperation of the security services. Secondly, there is often an unofficial command chain directly connecting these activities with high-level political leadership – in Google’s case, one unconfirmed report indicates that a single high-ranking government individual ordered the attacks, but ‘unofficially’ and without using state resources.¹⁹³ Finally, that most of the attacks are probably not directed against government systems but against private cooperation’s and their intellectual property. The final issue is difficult to overstate – while attacks on governments sometimes make their way into the media, attacks on private business hardly ever do. In the UK alone, cyberespionage supposedly costs business over GBP 16 billion (EURO 19 billion) a year.¹⁹⁴

As devastating as these attacks may seem, they do not amount to actual warfare if traditional Western legal definitions of warfare are used. Similarly, the **2007 Estonia** attacks have often been called everything for simple web-vandalism to all-out war. Over a period of three weeks, a number of significant attacks (the most visible of which were massive DDoS attacks) managed to disrupt a number of services provided by the government, banks, and news-outlets in Estonia. These attacks certainly

¹⁸⁹ Leigh, Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power*, Washington D.C., Brassey’s, Inc., 2004.

¹⁹⁰ Thornburg, Nathan, ‘Inside the Chinese Hack Attack’, *Time*, 25 August 2005, <http://www.time.com/time/nation/article/0,8599,1098371,00.html>.

¹⁹¹ See Arthur, Charles, ‘Google the latest victim of Chinese ‘state-sponsored’ cyberwar’, *Guardian*, 25 August 2005, <http://www.guardian.co.uk/technology/2010/jan/14/google-hacking-china-cyberwar>.

¹⁹² Winkler, Ira, ‘Guard against Titan Rain hackers’, *Computer World*, 20 October 2005, http://www.computerworld.com/s/article/105585/Guard_against_Titan_Rain_hackers.

¹⁹³ See Sawyer, Patrick, ‘Top Chinese officials ordered attack on Google, Wikileaks cables claim’, *The Telegraph*, 4 December 2010, <http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html>.

¹⁹⁴ See Allen, Darren, ‘Cyber-crime costs UK economy £27 billion per year’, *techwatch*, 17 February 2011, <http://www.techwatch.co.uk/2011/02/17/cyber-crime-costs-uk-economy-27-billion-per-year/>.

required a superlative effort on part of the Estonia and allied network professionals to contain, without which the damage would have been significantly worse.¹⁹⁵ The attacks were largely attributed to Russian hackers (see Russian section). According to the AF-SAB categorisation, these attacks may have been a nightmare for IT security professionals and led to significant disruption for the general population, however they would still not rank higher than a 'Level 1' attack – i.e. not really cyberwar at all. From a Critical Infrastructure point of view, however, the nation-wide disruption of services experienced in Estonia would certainly be a very major event.

Level 2: Equivalent to Kinetic Attack

While a case can be made that the disruptions in Estonia 2007 could possibly have been equivalent to a 'kinetic attack', the case is easier to make in the **Georgia 2008** cyberattacks. Launched in conjunction with the Russian military offensive against Georgia, the attacks ranged from propaganda attacks (defacement of websites) to denial of communications, and even potentially direct attacks on critical energy infrastructure. A number of open-source researchers have indicated that here, too, the likely culprits were a combination of volunteers and Russian cybercrime, at least tacitly supported or even organized by the Russian state security services.¹⁹⁶ There was clear cooperation of the cybercampaign with that of the Russian military forces,¹⁹⁷ and a clear military-political aim: to sever the ability of the Georgian government to communicate with its population and the world.¹⁹⁸ Compared with the attacks on Estonia, these were considerably more sophisticated and organized. Most importantly, they occurred in conjunction with traditional military operations, and therefore had a clear 'kinetic' effect.

A more certain candidate for 'Level 2 cyberwar' status are the purported Israeli attacks on a supposed Syrian nuclear facility in 2007. According to a number of reports, Israel may have used a variant of a suspected US cyberweapon called '**Senior Suter**' to disable the Syrian Integrated Air Defence Network prior to launching its airstrike.¹⁹⁹

Level 3: 'Malicious Manipulation'

Despite being the most serious types of cyberwarfare attack within the AF-SAB model, it is possible (depending, as always, on definitions) that the world may have already experienced Level 3 cyberwarfare attacks – at least, according to the AF-SAB definition. **Stuxnet** has been called a 'Cyber missile'²⁰⁰ directed squarely at the Iranian nuclear program by targeting its uranium enrichment capability. Specifically, Stuxnet manipulates the centrifuges and its associated SCADA control systems by feeding false data and orders into the system, leading to an unnoticed but steadily degrading of those systems through intentional damage. There has been clear evidence that Stuxnet was successful in damaging and delaying the Iranian enrichment program.²⁰¹ How significant a step-back this actually represents remains unclear. Equally unclear is who the perpetrators were, speculation has concentrated on Israel,²⁰² the United States,²⁰³ China,²⁰⁴ organized crime as well as Russia.²⁰⁵ Stuxnet, it needs to be

¹⁹⁵ see Espiner, 2008.

¹⁹⁶ See Project Grey Goose, 2009.

¹⁹⁷ Dancho, Danchev, 'Coordinated Russia vs Georgia cyber attack in progress', *ZDNet*, 11 August 2008, <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>.

¹⁹⁸ See US-CCU, 2009.

¹⁹⁹ Gasparre, Richard B., 'The Israeli 'E-tack' on Syria – Part I', *airforce-technology.com*, 11 March 2011, <http://www.airforce-technology.com/features/feature1625>.

²⁰⁰ See The Economist, *A cyber-missile aimed at Iran?*, 24 September 2010, http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

²⁰¹ See Farwell and Rohozinski, 2011.

²⁰² Ibid.

pointed out, was however not necessarily unique - according to one government expert, 'we have seen this type of thing before.'²⁰⁶

Stuxnet has not been often labeled a weapon of cyberwar (even though the term 'missile' certainly implies as much), possibly as it can only partially be described as an 'equivalent of a kinetic attack', the benchmark for a Level 2 attack. However, the earliest rumored cyberwarfare attack would have certainly made that grade. A former US Secretary of the Air Force and senior adviser to President Ronald Reagan has claimed that the CIA used a logic bomb in 1982 to destroy a Soviet gas pipeline. It 'was programmed to go haywire, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space.'²⁰⁷

²⁰³ See Broad, William J. et al., 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 January 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?ref=johnmarkoff>.

²⁰⁴ See Carr, Jeffrey, 'Stuxnet's Finnish-Chinese Connection', *Forbes*, 14 December 2010, <http://blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/>.

²⁰⁵ See Kay, David, 'As the worm turns', *The National Interest*, 1 October 2010, <http://nationalinterest.org/commentary/the-worm-turns-4168>.

²⁰⁶ Personal communication with author.

²⁰⁷ Reed, Thomas C., *At the Abyss: An Insider's History of the Cold War*, New York, Presidio Press, 2004, p. 269.

APPENDIX III: LIST OF MOST SIGNIFICANT CYBERATTACKS 2010²⁰⁸

January 2010: Google announced that an attack had penetrated its networks, along with the networks of more than 80 other US high-tech companies. The goal of the penetrations, which Google ascribed to China, were to collect technology, gain access to activist G-mail accounts and to Google's password management system. At the same time, Intel experienced a harmful cyberattack.

January 2010: Global financial services firm Morgan Stanley experienced a 'very sensitive' break-in to its network by the same hackers who attacked Google, according to leaked emails.

March 2010: A number of successful cyberattacks against NATO and European Union networks have increased significantly over the past 12 months, the international organizations revealed.

March 2010: Australian authorities say there were more than 200 attempts to hack into the networks of the legal defence team for executives from Australian energy company Rio Tinto, to gain inside information on the trial defence strategy.

April 2010: Hackers break into classified systems at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian defence and armament planning.

May 2010: A leaked memo from the Canadian Security and Intelligence Service says, 'Compromises of computer and combinations networks of the government of Canada, Canadian universities, private companies and individual customer networks have increased substantially. ... In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage.'

October 2010: Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems discovered in Iran, Indonesia and elsewhere, results in significant physical damage to the Iranian nuclear program.

October 2010: The Wall Street Journal reports that hackers using Zeus malware, available in cybercrime black markets for about \$1,200, were able to steal over \$12 million from five banks in the United States and Britain.

December 2010: British Foreign Minister William Hague reported last month attacks by a foreign power on the British Foreign Ministry, a defence contractor and other British interests. The attack succeeded by pretending to come from the White House.

January 2011: The Canadian government reports a major cyberintrusion involving the Defence Research and Development Canada, a research agency for the departments of National Defence Finance and the Treasury Board, Canada's main economic agencies. The intrusions forced the Finance Department and the Treasury Board to disconnect from the Internet.

²⁰⁸ Prepared for by James Lewis, CSIS, for the US Congress Homeland Security Committee, March 2011. List reproduced with assistance of http://www.bankinfosecurity.com/articles.php?art_id=3440

APPENDIX IV: CHINA: MILITARY, NETIZENS AND PATRIOT HACKERS

Few countries have concentrated on 'cyber' as much as China. In part this derives from the 'Gulf War shock' of 1991, in which the US military showed its total dominance in conventional warfare. Within this context, the Chinese military establishment has pursued cyberwarfare capabilities as an attempt to build an 'asymmetric counter' to this clear conventional US military advantage. At the same time, the US is seen as also having the most advanced cyber-capabilities, and that these directly threaten China, who often proclaims it to be the biggest victim of cyberattacks.²⁰⁹ Further, the explosive economic growth of China (to say nothing of the Internet itself) has profoundly affected the country. From the mid 1990s China has gone from around 1 million computers and virtually zero online communities to around 300 million computer and around 420 million Internet users.²¹⁰ This huge population of 'Netizens' ('people of the net') represent a major security concern for the Chinese Communist Party.

Chinese theory on Cyberwar include a supposed doctrine for the Chinese equivalent of the US Network Centric Warfare concept entitled 'Integrated Network Electronic Warfare' (INEW), concepts surrounding mass mobilization of civilian resources known as 'People's War', and attempts to define a strategic level of conflict – 'Information Warfare'. In a widely-reported publication called 'Unrestricted War', two PLA officers emphasized that the future of conflict will be about blurring the line between civilian and military resources to exercise control of information in all manifestations, and namely *that the best way to achieve victory is to control, not to kill.*²¹¹ Thus defined, Information Warfare (of which Information Operations is simply an operational subset) has also been formalized within a 'Three Warfares' concept, encompassing 'Media Warfare', 'Psychological Warfare', and 'Legal Warfare'.²¹²

China's governmental cyberwar capabilities are strong and increasing – the '2011-2015 Five Year Plan' makes a clear commitment to the expansion of these capabilities.²¹³ The capabilities cover a number of different tasks. At the strategic level, the PLA General Staff Department (especially the 3rd and 4th department, as well as the 7th Bureau of the Military Intelligence Department) probably maintains the capability to wage strategic cybercampaigns against foreign adversaries, and defend against such attacks. The foreign-intelligence Ministry of State Security (MSS) is purported to be behind a number of cyberespionage campaigns. According to US reports, China has developed a (battalion-sized) group of specialists in 'strategic cyberwarfare' (which includes attacks on an enemy's national critical infrastructure) that have been dubbed 'Net Force'.²¹⁴ On the operational, field-army level, a number of IO units have been set up within Group Armies and Military Districts, although there are clear differences between those of the regular army, the reserves, and the militia. It has been widely reported that the PLA has integrated 'Information Warfare' and 'Information Operations' (IW/IO)²¹⁵ units in its standard field-army organization structure from 2003 onwards²¹⁶ (the first exercises supposedly

²⁰⁹ See Lam, Willy, 'Beijing beefs up cyber-warfare capacity', *Asia Times Online*, 9 February 2010, <http://www.atimes.com/atimes/China/LB09Ad01.html>.

²¹⁰ See Internet World Stats, 2010.

²¹¹ See Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare: China's master plan to destroy America*, Panama City, Pan American Publishing Company, 2002.

²¹² For a comprehensive study of the 'Three Warfares' Study' see Walton, 2010.

²¹³ See Lam, 2010..

²¹⁴ See Kanwal, Gurmeet, 'China's Emerging Cyber War Doctrine', *Journal of Defence Studies*, vol. 3(3), July 2009, pp. 14-22, http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf.

²¹⁵ Although a literal translation, the actual meaning is that of 'Information Operations', with however one exception – 'Information Warfare operations' are also conducted in times of peace. Therefore IW units can operate in peacetime, and in wartime would have dedicated IO duties. In western parlance however these are simply considered IO units.

²¹⁶ Zhou, Ye, 'Jiefangjun Zixunhua budui jinnian chengjun' (PLA Cyberwarfare units deployed this year), *Zhongguo Shibao*, March 15 2003, <http://news.chinatime.com>.

occurred already in 1998).²¹⁷ There are indications that the field level active and reserve units support conventional military capabilities, while the independent militia units are intended more for a 'strategic strike'(such as on an enemy's critical infrastructure) and could operate independently from the military command.

Primary Agencies	Subordinate Agencies	Unattributed Agencies
General Staff Dep. (2,3,4)	National Watch Center	MIIC
PLA	SIGINT / ELINT stations	NAPSS
PLA Militia	"Net Force"	China Telecom
PSB	"Cyber Security Force"	U/I „Web Censor“ Org
MSS	CNCERT	U/I Universities
	PLA IW (C4SIR?) „Brigades“	
	Militia IO Units	

The Chinese defensive cyberwar capabilities – their cybersecurity capabilities – are very strong. A number of CCP bodies probably have offensive and defensive cyber-missions, for instance within the CCP Central Propaganda Department.²¹⁸ China has gone to great lengths to protect its government systems from attack, including developing its own PC desktop operating system (called 'Kylin') and even Desktop CPU processor (called 'Longxin' or 'Godson') to 'harden' their networks – something no other country has done to this extent. Further, the 'Great Firewall' web censorship regime (known as the 'Golden Shield'), has considerable capabilities to block and filter Internet traffic, both inside China and abroad.²¹⁹ Also, the 'Great Firewall' system has the ability to disrupt Internet communication globally – in 2009/2010, supposed 'errors' of the system led to the possibility of major portions of the worldwide Internet traffic being temporarily routed via China and through the 'Great Firewall', severely compromising the integrity and confidentiality of the global Internet.²²⁰ The human investment in the Great Firewall is considerable as well, around 30,000 - 50,000²²¹ people are supposedly engaged in online censorship of blog posts, messages, emails, and even mobile-phone text messages.

The Internet has achieved unparalleled importance in Chinese society, and represents one of the few outlets for dissent or political expression. The Internet and the blogosphere represent a considerable challenge to Chinese Communist Party rule. While China only has a limited civil society, it does have the most active 'netizens', or participants in cybersociety, in the world, as well as the greatest number of Internet users by far: according to some reports, China now has over 50 million bloggers.²²² These bloggers, together with the very wide and active 'Patriot Hacker' community, quite clearly represent one of the most significant potential reservoirs of 'subversive' behaviour.

The central government probably attempts to 'co-opt' these potential subversives through a wide range of programs intended to bind these individuals to the state. It was recently reported that Beijing

²¹⁷ Daily Herald, *Information Warfare*, 20 August 2001, <http://www.b66.info/InformationWarfare.htm>.

²¹⁸ US-China Economic and Security Review Commission, 2009.

²¹⁹ See, for instance, August, Oliver, 'The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online', *Wired*, 23 October 2007, http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall.

²²⁰ See, for instance, Part 1.2 of this study; and BGPmon, 2010.

²²¹ Canwest News Service, *Great Firewall China's answer to borderless Internet*, 13 January 2007, <http://www.canada.com/topics/news/world/story.html?id=45f6e905-5aab-4af4-8736-cf59a24b664b&k=70987>.

²²² Sachoff, Mike, 'Chinese Bloggers Reach 50 Million', *WebProNews*, 7 January 2009, <http://www.webpronews.com/topnews/2009/01/07/chinese-bloggers-reach-50-million>.

maintained a programme to finance bloggers 'at times of public-opinion crises'.²²³ There are supposedly as many as 30,000 such agents, all paid by the government, and apparently including some of the most well-known and trusted 'dissident' bloggers.²²⁴ The PLA militia and reserve system is another important avenue for co-opting netizens. Moreover, through programs such as the National Defence Reserve Forces, many of China's technical (and particularly information-technology) students are automatically considered to be part of the Chinese defence organization. A number of the identified reserve and militia IO units are located at universities as well as state enterprises. In one example reported as far back as 2003, the Guangzhou City militia built up a dedicated IW battalion organized around a provincial telecommunications company.²²⁵

Chinese 'Patriot Hacker' gangs have likely been behind the majority of visible attacks directed against Western governments and the private industry – attacks that in the very least are tolerated, if not necessary directed, by the state. The cybersecurity company iDefence has tracked over 250 identified hacker groups in China.²²⁶ Some of these hacker groups claim a gigantic membership – the largest, the Red Hacker Alliance, has claimed (somewhat implausibly) to have 400,000 members.²²⁷ Many of the hacker groups have participated in PLA-organized hacker competitions which are often directed against Western targets, the winners of which are rewarded with monthly cash stipends from the military.²²⁸ These groups can be very proficient, and a real threat to Western governments - in 2007, the Pentagon alone had between 25 and 27 terabytes of data (over 5,000 DVDs worth) exfiltrated from their systems.²²⁹ According to a FBI expert, the majority of these attacks nevertheless are not coordinated with the government, and that the government interactions occur 'completely informally'.²³⁰ The system puts process before outcome or collection over analyses,²³¹ meaning that most of the large network-exploitation attacks are highly opportunistic and not really connected to the Chinese leadership's overall intelligence-gathering priorities or cyberwarfare plans. This does not mean that unofficial Chinese cyber-capabilities do not directly or indirectly support the aims of the Chinese government. For Beijing the primary aim of integrated national capability is not offensive but defensive: an attempt at 'internal pacification' of potential subversives.

²²³ MacKinnon, Rebecca, 'China Tightens Internet Controls in the Name of Fighting Porn, Piracy, and Cybercrime', *RConversation*, 14 December 2009, <http://rconversation.blogs.com/rconversation/2009/12/china-tightens-internet-controls-all-in-the-name-of-fighting-porn-piracy-and-cybercrime.html>.

²²⁴ Liu, Melinda, 'Blog the Record Straight', *Newsweek*, 28 February 2009, <http://www.newsweek.com/id/186996>.

²²⁵ Thomas, 2004.

²²⁶ US-China Economic and Security Review Commission, 2009.

²²⁷ See Minnick, Wendell, 'Is Beijing Behind Cyberattacks on the Pentagon?', *DefenceNews*, 2 June 2008, <http://www.defencenews.com/story.php?i=3576373&c=FEA&s=SPE>.

²²⁸ For more on the Chinese hacker scene see Klimburg, 2011(a).

²²⁹ US-China Economic and Security Review Commission, 2009.

²³⁰ *Ibid.*

²³¹ *Ibid.*

APPENDIX V: RUSSIA: SILOVIKI, CYBERCRIME AND HACKER PATRIOTS

Russia's cyber-capabilities and doctrine have received less emphasis in the public than Chinese attacks, partly since there is considerably less open-source information for observers to comment on. However, Russia's cyber-capabilities are considered to be 'nearly as good as the US ones', according to a statement by General Keith Alexander, head of USCYBERCOM.²³² Russia's capabilities in this field derive from a deep tradition in both 'Information Warfare' and PSYOPS doctrine as well as the strong position of the intelligence services within the state – in 2006 it was reported that up to 78% of 1,016 leading political figures in Russia had previously served in organizations affiliated with the KGB or FSB.²³³ These capabilities are also based on the strong technical skills within the general population, which produces some of the best IT staff, as well as the most advanced cybercriminal syndicates, in the world.²³⁴

Russian information security thinking is said to be derived from the long-standing Soviet interest in strategic PYSOPS (Psychological Operations), which, unlike in the West, operates on a strategic level as well as on an operational level. First defined over 30 years ago by V. A. Lefebvre, the concept of 'reflexive control' is considered to be 'a process by which one enemy transmits the reasons or bases for making decisions to another.'²³⁵ In other words, to completely dominate an adversary's decision-making process through various tools, including, for instance, semantics. According to this paradigm, Russia is under constant threat of being dominated by American 'information control', both directly in cyberspace²³⁶ as well as more obliquely, through the 'Western influence' on the Russian civil society.²³⁷ The Information Security doctrine of the year 2000 makes repeated reference to the importance of protecting Russian 'spiritual renewal' from foreign influences.^{238,239} On an operational level, Russian 'Information Operations' thinking is highly developed and is segmented according to 'Information Psychological' and 'Information Technical' means.²⁴⁰ The Russian military has remarked on the desirability of using proxy organizations to wage cyberwarfare disguised as simply cybercriminal or cyberterrorist activity.²⁴¹

The Russian governmental cyberwarfare capabilities are probably concentrated within intelligence and intelligence-related structures. The main internal security service FSB is presumed to have the farthest-reaching cyberwarfare components. The three main organizational units are all directly subordinated to headquarters: the 'Information Security Centre' is certainly the most visible and probably the most important – its members are often quoted when discussing Information Assurance. It has a directorate rank and therefore is likely to have over 55 employees.²⁴² It is also the contact point (or managing body) of RU-CERT, the officially independent Russian CERT. Many other FSB offices of equal rank also play a role: the Communications Security Centre, which was taken over from the former signal intelligence agency FAPSI (now known as SSSI), is supposedly one of the most high-tech Centres in the security

²³² See posting of Beowulf, 'Cyber Threat to Pentagon is Global: China, Russia Near Peers of US', *osint*, 1 October 2010, <http://www.mail-archive.com/osint@yahoogroups.com/msg62329.html>.

²³³ Albats, Evgenia, 'Siloviks in Power: Fears or Reality? – Interview with Olga Kryshstanovskaya', *Echo of Moscow*, 4 February 2006 (currently unavailable).

²³⁴ See Jellenc, Eli and Zenz, Kimberly, 'Global Threat Research Report: Russia', *An iDefence Security Report*, 10 January 2007, <http://www.verisign.com/static/042139.pdf>.

²³⁵ Thomas, 2004.

²³⁶ Molchanov, N.A., 'Information Resources of Foreign States as a Threat to Russia's Military Security', *HighBeam*, 1 October 2008, <http://www.highbeam.com/doc/1G1-194154588.html>.

²³⁷ Thomas, 2004.

²³⁸ GlobalSecurity, *Russian Military Doctrine*, <http://www.globalsecurity.org/military/world/russia/doctrine.htm>.

²³⁹ See the Doctrine of the Information Security of the Russian Federation; available at: <http://www.embrusscambodia.mid.ru/doc-information-e.html>,

²⁴⁰ Bikkenin, 2003.

²⁴¹ Russian Federation Military Policy in the Area of International Information Security, 2007.

²⁴² Agentura, *Structure of the FSB*, <http://www.agentura.ru/english/dosie/fsb/structure/>.

services. The Special Events Service, the Directorate of Special Communications, Directorate of Communications Security, and the Directorate of Assistance Programs presumably also all have a cyber-role. Other important agencies directly attached or subordinated to the FSB include the 'National Anti-Terrorist Committee'²⁴³ and the 'National Anti-Terrorist Centre' (the 'Special Centre') and the 'Centre for Licensing, Certification, and Protection of State Secrets' ('LSZ Centre'). The 'Special Centre' has been particularly active in recruiting Russian 'hacker patriots' (see below) and has an extensive reach, due to its broad 'anti-terrorism' mandate. The Kremlin security organizations (in particular the FSO) have also been purported to have cyber-capabilities.²⁴⁴ The Russian military in general and the military intelligence GRU in particular, are also said to have an active role in cyberwarfare.²⁴⁵

Primary Agencies	Subordinate Agencies	Unattributed Agencies
FSB	Info Sec Center	STC Atlas
FSO	NAK - "Special Center"	Rostelekom (et al.)
GRU	"LSZ Center"	Nashi, EYM, et al.
MVD	Coms Sec. Center	
	SSSI	
	GUSTM	
	RU-CERT	

While China is said to emphasize 'content control' of the Internet, Russia clearly emphasizes 'network control.'²⁴⁶ Uniquely, Russia maintains the ability to completely monitor all Internet traffic within its jurisdiction, with the SORM-2 legislation requiring all Internet Service Providers to install the necessary technology on their systems. Russia also recently announced that it would develop its own alternative to the Windows operating system, largely due to its security concerns.²⁴⁷

In the majority of purported Russian origin cyberattacks it is very likely that cybercriminals played a substantial role, often as providers of 'logistic services' to gangs of politically motivated hackers – so called 'hacker-patriots.' Many public reports have pointed to the role of the Russian Business Network (RBN), described by *The Economist* as the world's foremost cybercrime organization, as a provider of the logistic basis for cyberattacks.²⁴⁸ RBN is identified by international security and law enforcement communities as a major threat.²⁴⁹ Some 40% of global cybercrime in 2007 was said to be directly due to RBN.²⁵⁰ It was the world's foremost spammer, child-pornography distributor and producer of malware and phishing software. It delivered these services in part through various botnets, including the then world's largest (*Storm*), which in 2008 was responsible for 20% of all spam e-mail globally, and provided

²⁴³ Heickerhö, Roland, 'Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations', *Swedish Defence Research Agency*, March 2010, <http://www2.foi.se/rapp/foir2970.pdf>.

²⁴⁴ Ibid.

²⁴⁵ Ibid.

²⁴⁶ Thomas, 2004.

²⁴⁷ See Weir, Fred, 'Russia to drop Microsoft in quest for 'national' operating system', *The Christian Science Monitor*, 29 October 2010, <http://www.csmonitor.com/World/Europe/2010/1029/Russia-to-drop-Microsoft-in-quest-for-national-operating-system>.

²⁴⁸ See *The Economist*, *A Walk on the Dark Side*; *Economist*, 30 August 2007, http://www.economist.com/displaystory.cfm?story_id=9723768.

²⁴⁹ Newsweek 2009.

²⁵⁰ Blakely, Rhys et al., 'Cybergang Raises Fear of New Crime Wave', *The Times*, 10 November 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece; Warren, Peter, 'Hunt for Russia's Web Criminals', *Guardian*, 15 November 2007, <http://www.guardian.co.uk/technology/2007/nov/15/news.crime>.

these and many other services to cybercriminals and hacker patriots. The network has also been accused of facilitating the attacks on Georgia in July–September 2008.²⁵¹ While the main RBN front organizations were supposedly shut down by Russian authorities and went largely offline in 2007, the network is said to have reconstituted abroad in a number of new organizations, and in 2010 it is still estimated as having a yearly turnover of over USD 2bn.²⁵² Prior to 2007 there were numerous indications that RBN enjoyed at least the tacit support of the Russian security services.²⁵³ Overall, much of Russian society sees these activities – cybercrime directed towards the West – as a form of ‘gentlemen’s misdemeanour’, or sometimes even in positively heroic terms. The courts – and especially the security services – seem to echo this opinion. Individuals indicted in cybercrimes have mysteriously had their charges dropped, and even reappeared in positions advising the Russian government.²⁵⁴

The Russian security services often attempt to co-opt or recruit cybercriminals and hacker patriots.²⁵⁵ Many of the latter operate against ‘anti-Russian forces’ with the support of the security services. Attacks by hacker patriots against ‘pro-Chechen’ websites in 2002–04 were described by the Tomsk FSB office as not being illegal and simply an ‘expression of their political position, which is worthy of respect’.⁴¹ The Tomsk FSB office is able to draw on students from Russia’s top computer-science university who themselves have been accused of a host of activities, including instigating the theft of emails and other data from scientists at a British university 2009 to support Russia’s interests at the Copenhagen climate summit that year.²⁵⁶ Other reports have indicated that the National Antiterrorist Committee (NAK) has tried to pressure these non-state hackers into collaborating with it.²⁵⁷

There have also been clear indications that Kremlin-aligned youth groups, such as Nashi and the far-right Eurasian Youth Movement have conducted cyberattacks on their declared enemies, usually abroad. For instance, Konstantin Goloskov, a Nashi ‘commissar’ and assistant to Sergei Markov, a member of the Duma, claimed credit for organising the 2007 attacks on Estonia.⁴⁵ Goloskov said the attacks were ‘purely a reaction from civil society ... and, incidentally, such things will happen more and more’.²⁵⁸

²⁵¹ INFRAGARD, *The Russian Business Network: Attacking Georgia and Stealing from Americans*, 11 March 2009, http://www.nationalstrategies.com/pdf/publicSafety_GovSec_RussianBusinessNetwork.pdf. However, other reports have indicated that the Georgian attacks were directly attributable to the Russian security services mimicking RBN networks. See, for example, Project Grey Goose, 2009.

²⁵² Verneti, Gianmaria, ‘The Power of Networking: An Insight on the Russian Business Network’, *Bright*, 1 July 2010, http://flarenetwork.org/report/enquiries/article/the_power_of_networking_an_insight_on_the_russian_business_network.htm.

²⁵³ Warren, 2007.

²⁵⁴ See Krebs, Brian, ‘Following the Money: Rogue Anti-virus Software’, *The Washington Post*, 31 July 2009, http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html; for an open letter by the Russian State Duma, on the subject of Chronopay, see Ponomarev, I. V., <http://krebsonsecurity.com/wp-content/uploads/2010/05/ivptrans.pdf>.

²⁵⁵ See Klimburg, 2011(a).

²⁵⁶ Rainsford, 2010; and Walker, 2009.

²⁵⁷ See Klimburg, 2011(a).

²⁵⁸ See Coalson, Robert, ‘Behind The Estonia Cyberattacks’, *Radio Free Europe/Radio Liberty*, 6 March 2009, http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html.

APPENDIX VI: THE US: CYBEROPS, PRIVATE BUSINESS, AND 'WHITE HATS'

The United States maintains the most advanced and sophisticated cybersecurity organizations in the world. Numbers are very difficult to obtain, but the (classified) budget of the headline Comprehensive National Cybersecurity Initiative (CNCI) for the entire US federal government is expected to amount to over USD 30 billion for the period 2009-2013,²⁵⁹ which itself only represents additional funding. According to one estimate, the US Federal government spends around USD 10 billion every year on cybersecurity, without local or state programs or the CNCI considered.²⁶⁰ If these numbers are true, it is likely that US spending on cyber dwarfs that of all other countries worldwide, together. Within the US military alone there might be as many as 88,000 people involved in 'Information Operations' – even if 'true hackers' would only account for a fraction of this number.²⁶¹ However, the vast majority of US cybersecurity measures are probably defensive – primarily focused at protecting the vast US governmental communication networks, and, to a much lesser extent, the national Critical Infrastructure.

US thinking on cyberwarfare and cybersecurity is broad and steadily evolving. The US military developed an interest earliest: the Air Force Information Warfare Centre (AFIWC) was set up already in 1993, while the first reports encompassing civilian policy on the 'cyberdimension' appeared in 1997²⁶² and the first relevant Presidential Decision Directives in 1998.²⁶³ Between 1998 and 2010 a number of high-level policy documents were published, however major issues still remain to be addressed. Despite having the longest (and arguably most intense) discussion on 'Information operations' and 'Cyberspace', the US does not have a clearly identifiable integrated Cyber-concept. The four current capstone (leading) documents illustrate the difficulty: the Joint Publication 3-13 (JP 3-13) 'Joint Doctrine for Information Operations' of the Joint Chiefs of Staff (revised 2006), the 'National Military Strategy for Cyber Operations' (NMS-CO, 2006), the 'Cyberspace Policy Review' of the White House (2009), and the 'Comprehensive National Cyberspace Initiative 2009' (CNCI) seem to have little in common, despite each being the primary document for the military (operational and strategic) and political cyber-community, respectively. They do not even have a common terminology. Although the term 'cyberwarfare' is enjoying increasing prominence even in military circles, '[t]here is no definition of Cyberwarfare, no policy on how and when Cyber weapons should be deployed and used, and we do not have a clear idea of who our enemies are', according to a former White House cybersecurity advisor.²⁶⁴

US cybersecurity-thinking can be broadly segmented along two differing schools of thought on the policy level, namely 'cyber-deterrence' and 'resilience', and an underlying military-defined operational approach to cyber-operations. In NMS-CO US military officially adopted cyberspace as the fifth 'domain' – after air, land, sea and space. The military's thinking has concentrated primarily on two operational tasks: the defence of the US defence communications networks (in particular the all-encompassing Global Information Grid and associated sub-networks) and the support of 'conventional' military missions. The latter mission, traditionally the domain of the US Air Force, has a strong lineage arising

²⁵⁹ See Gorman, Siobhan, 'Hathaway to Head Cybersecurity Post', *The Wallstreet Journal*, 8 February 2009, <http://online.wsj.com/article/SB123412824916961127.html>.

²⁶⁰ See Drew, Christopher and Markoff, John, 'Cyberwar, Contractors Vie for Plum Work, Hacking for U.S.', *The New York Times*, 31 May 2009, <http://www.nytimes.com/2009/05/31/us/31cyber.html>.

²⁶¹ See Ibid.

²⁶² Commission on Critical Infrastructure Protection, *Toward Deterrence in the Cyber Dimension*, 1997, http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf.

²⁶³ Presidential Decision Directive/PDD-63, *Critical Infrastructure Protection*, <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

²⁶⁴ GCN, *Cybersecurity: U.S. Must Craft Cyberwarfare Battle Strategy*, 18 February 2008, <http://www.gcn.com/Articles/2009/02/18/Black-Hat-Federal-Kurtz.aspx?Page=2>.

from within Electronic Warfare (EW) and Signal Intelligence (SIGINT). Modern 'cyberweapons', for instance a purported EW System known as 'Senior Suter', are supposedly able to hack into air defence networks using an enemy's own radar signal to gain access,²⁶⁵ rather than needing an Internet connection. A similar system was purportedly used by the Israeli Defence Forces to subvert the Syrian Air Defence Network in 2007, allowing Israeli planes to bomb a supposed Syrian nuclear weapons site.²⁶⁶ At the same time, there are indications that 'strategic strike' (i.e. the ability to comprehensively attack an enemy's critical infrastructure through cyber-means) have not featured highly in US military thought. Most of the thinking seems to revolve around cyber-support for military operations, rather than the execution of strategic-strike operations through cyber-means on their own, as is clearly implied in both Russian and Chinese Information Warfare thinking.²⁶⁷ The US military seems to discount the possibility of a cyberwar being waged only online, with no 'kinetic' attacks accompanying it. One senior US cyberwarrior quoted noted technologist Bruce Schneier in saying 'If we are at cyberwar, we will be at war – other things will be happening as well.'²⁶⁸

On the policy level, two strong (not always opposing) schools of thought have manifested themselves. The school of 'cyberdeterrence'²⁶⁹ maintains that the best defence the US can have against cyberattack are strong offensive capabilities capable of inflicting unacceptable cost on any potential attacker. These costs can be imposed via cyberattack but, more importantly, through striking back with other elements of 'national power' (summarized with 'DIME' - Diplomacy, Informational, Military, and Economic). More recently under the Obama administration,²⁷⁰ the concept of 'resilience', long an important part of Critical Infrastructure Protection (CIP), is increasingly being referred to on a policy level.²⁷¹ 'Resilience' (which can be defined as the ability of a system to withstand shocks due to proactive risk reduction, slack, redundancy measures and rapid recovery) is essentially a defensive-orientated strategy that intends to limit disruptions and the consequences of disruptions due to cyberattacks. Resilience as a concept seems well suited to deal with the 'cyberveil', i.e. the attribution problem, an unanswered issue within the 'deterrence' strategy – striking back is problematic when the attacker is unknown. Resilience is also a broad-based security concept that is already well accepted in other international security fields. At the same, it must be stated that, as a broad based concept, Resilience in the US could potentially be instrumentalized by special interest groups, both for seeking commercial gain as well as expanding legal mandates.

US (federal) cyber-capabilities are heavily segmented according to tasks assigned in the US Constitution.²⁷² This segmentation is partly responsible for the plethora of US organizations dedicated to cybersecurity (in whatever form). The number of US organizations with clear cyberwarfare-relevant cybersecurity missions is considerable, and even an overview cannot be realistically attempted here. In general, it can be said that the vast majority of these organizations have clear Computer Network Defence missions, rather than being focused on offensive cyberwar. While the strong defensive focus is partially a result of the strong US reliance on communications technology (also a centrepiece of the

²⁶⁵ Clarke and Knake, 2010.

²⁶⁶ See *ibid.*, or, for instance, Defence Update, *SUTER V. Cyberworld's Black Knights*, http://defence-update.com/features/2008/may08/suter_v.htm.

²⁶⁷ There are considerable differences in definitions regarding the use of the term 'Information Warfare' (see Part 1).

²⁶⁸ See, for instance, Schneier, Bruce, *The Threat of Cyberwar Has Been Grossly Exaggerated*, http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.

²⁶⁹ See, for instance, Libicki, 2009.

²⁷⁰ See, for instance, Corbin, 2010.

²⁷¹ See, for instance, *ibid.*

²⁷² These include Title 6 (Domestic Security), Title 10 (Armed Forces), Title 18 (Crimes and Criminal Procedure), Title 32 (National Guard), Title 40 (Public Buildings, Property, and Works) and Title 50 (War and National Defence) see NSMC-CO Appendix A <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf>.

Network Centric Warfare doctrine), a further reason is simply a strong tendency towards 'silofication' within government bodies, meaning that every department requires its own defensive organization.

Primary US Federal Government Cybersecurity organizations (selection)		
CCIPS (DoJ)	JIOWC (STRATCOM)	NetOps Centers (DISA)
NCSD (DHS)	D3 (DISA)	NCDOC (USN -10th Fleet)
NCCIC (DHS)	A-GNOSC (US Army)	FIWC (USN-10th Flcct)
USCERT (DHS)	Regional / Theater NOCs (US Army)	MCNOSC (USN/Marines)
Cyber Division (FBI)	67 th NetWar Wing (USAF -24 th AF)	166 th NWS (Air Nat Guard)
IC3 (FBI)	2x INOSCs (USAF -24 th AF)	262 nd IAS (Air National Guard)
CATs (FBI)	624 th Operations Center	177 th IAS (Air National Guard)
CIRG (FBI)	687 th IO Wing (USAF-24 th AF)	N-TOC (NSA/CSS)
NCI-JTF (FBI)	688 th IO Wing (USAF-24 th AF)	IC-IRC (DIA)
JIOC (USCYBERCOM)	689 th IO Wing (USAF-24 th AF)	(Defense Information Agency)
JTF-Cyber (USYBERCOM)	6x ASOCs (+ Global Strike) (USAF)	(US Secret Service)
JFCC-NW (USCYBERCOM)	AFIOC (USAF)	(Central Intelligence Agency)

Overall the US cybersecurity mission is relatively fragmented. In theory, the DHS has responsibility for all .gov networks as well coordination of the Critical Infrastructure and Key Resources (CIKR) mission, while USCYBERCOM (a US Department of Defence and National Security Agency organization) is responsible for the .mil networks as well as all 'national security' cybertasks. In practice there are considerable exceptions and grey areas, for instance the Department of Defence maintains its own CIP Program by protecting the so-called Defence Industrial Base. The DHS, on the other hand, had until recently (2011) little resources and a very limited mandate. Recently, the DHS has started to work closely with the DoD on CIP issues,²⁷³ something that was previously unthinkable due to the highly segmented nature of US cyberresponse policy. Until 2010 effective cyber crisis-management in the US was largely dependent on the 'identity of the aggressor', something that would probably have been difficult to determine at the time of an attack. The US has however recently advanced considerably in its 'Whole of Government' cybersecurity capabilities. The new National Cyber Incident Response Plan (and relevant organizations such as NCCIC²⁷⁴) was a major step forward, and is very significant increase of US Cyberdefense capability.

US non-state cyber-capabilities are by far the most significant in the world, albeit much less integrated with government capabilities than in Russia or China. It is worth remembering that the majority of all cybersecurity-relevant activities generally occur outside of government control. The private sector is responsible for most of the software and hardware that is exploited for cyberattacks, maintains much of the network infrastructure that these attacks are conducted over, and often owns the Critical Infrastructure that these attacks are directed against. Further, civil society actors – as distinct from the private sector – dominate cyberspace, defining the programmed parameters (i.e. the software protocols) of the cyber-domain, as well as executing, researching, and ultimately, publicly speculating on cyberattacks. Together, these non-governmental actors account for the bulk of what is termed 'national' cybersecurity in most Western nations, and especially in the United States.

The Defence Industrial Base (DiB) similar private contractors operate very closely with the US government. Many of the 850,000 holders of a Top Secret clearance are not part of government but the

²⁷³ See Chabrow, 2010.

²⁷⁴ National Cybersecurity and Communications Integration Centre (NCCIC) – a large, 24-hour, DHS-led coordinated watch and warning centre with particular national cyberdefence crisis management tasks.

private sector.²⁷⁵ They however often maintain critical cybersecurity and even intelligence gathering capacities, and from outside can be indistinguishable from government. While the overall US CIKR program is much less integrated than the DoD DiB program, thousands of individuals within key private companies and similar organizations receive classified government briefings, and are constantly adjusting to the full range of cyberattacks on their systems. Even outside of these specialized information exchanges and Public-Private Partnerships (PPP), private companies have a dominant role in cybersecurity. Software companies such as Microsoft and Adobe constantly seek to patch holes in their software programs through which attacks are launched, and these attacks are usually discovered by dedicated security companies such as McAfee or others.

The highly important role of civil society is often not well understood, despite the fact that much of the Internet was effectively built (and continues to be maintained) by volunteers, such as at the Internet Engineering Task Force.²⁷⁶ So-called ethical or 'white-hat' hackers have often quite literally 'saved' the Internet from collapse,²⁷⁷ usually with no remuneration whatsoever. Finally, a number of all-volunteer policy and research organizations have conducted in-depth investigations of cyberattacks, including Stuxnet (by the Cybersecurity Forum Initiative - CSFI)²⁷⁸, Russian cyberattacks (Project Grey Goose – Intelfusion)²⁷⁹ and Chinese cyberattacks (Information Warfare Monitor).²⁸⁰ The information in these reports was the basis for much of the Western media speculation as to the origin of the attacks, and probably also played a role in addressing the 'root actors' involved. Perhaps most crucially, these actors attempt to lift the 'cyberveil' that attackers hide behind, and can thus contribute to a kind 'deterrence' of their own.

²⁷⁵ Priest and Arkin, 2010.

²⁷⁶ Borsook, 1995.

²⁷⁷ See Klimburg, 2011(a).

²⁷⁸ See for instance <http://www.csfi.us/?page=stuxnet>

²⁷⁹ See Project Grey Goose 2008.

²⁸⁰ Information Warfare Monitor is located at the Munk School of Global Affairs at the University of Toronto has traced number of these attacks, most famously 'GhostNet' and 'Shadows in the Cloud'.

APPENDIX VII: EU M.A.D.R.I.D. REPORT TIMETABLE FOR CYBER

Cybercrime and Network and Information Security		
Actions	Responsible	Timetable
<i>Measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as the one on modernised Network and Information Security Agency (ENISA) as well as other measures allowing faster reactions in the event of cyberattacks</i>	<i>Council Commission European Parliament</i>	<i>2010-2012</i>
<i>Legislative proposal on attacks against information systems</i>	<i>Commission</i>	<i>2010</i>
<i>Creation of a cybercrime alert platform at European level</i>	<i>Europol Commission</i>	<i>2010-2012</i>
<i>Develop a European model agreement on public private partnerships in the fight against cybercrime and for cybersecurity</i>	<i>Commission</i>	<i>2011</i>
<i>Measures, including legislative proposals to establish rules on jurisdiction on Cyberspace at European and International levels</i>	<i>Commission</i>	<i>2013</i>
<i>Ratification of the 2001 Council of Europe Cybercrime Convention</i>	<i>Member States</i>	

BIBLIOGRAPHY

- Albats, Evgenia, 'Siloviks in Power: Fears or Reality? – Interview with Olga Kryshtanovskaya', *Echo of Moscow*, 4 February 2006 (currently unavailable).
- Allen, Darren, 'Cyber-crime costs UK economy £27 billion per year', *techwatch*, 17 February 2011, <http://www.techwatch.co.uk/2011/02/17/cyber-crime-costs-uk-economy-27-billion-per-year/>.
- Ang, Peng Hwa, 'Self Regulation after WGIG', in Drake, William J. (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, New York, UNICTTF, 2005, pp. 129-34, <http://www.wgig.org/docs/book/toc2.html>.
- ANSSI, *Exercice PIRANET 2010: l'État s'entraîne à faire face à une attaque de grande ampleur sur les systèmes d'information*, 25 June 2010, http://www.ssi.gouv.fr/site_article248.html.
- Arthur, Charles, 'Google the latest victim of Chinese 'state-sponsored' cyberwar', *Guardian*, 25 August 2005, <http://www.guardian.co.uk/technology/2010/jan/14/google-hacking-china-cyberwar>.
- August, Oliver, 'The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online', *Wired*, 23 October 2007, http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall.
- Averill, Bruce and Luijif, Eric A.M, 'Canvassing the Cybersecurity Landscape: Why Energy Companies Need to Pay Attention', *Journal of Energy Security*, 18 May 2010, http://www.ensec.org/index.php?option=com_content&view=article&id=243:canvassing-the-cyber-security-landscapewhy-energy-companies-need-to-pay-attention&catid=106:energysecuritycontent0510&Itemid=361.
- BBC, *Cyber crime tool kits go on sale*, 4 September 2009, <http://news.bbc.co.uk/2/hi/technology/6976308.stm>.
- Beal, Vangie, 'The Difference Between a Computer Virus, Worm and Trojan Horse', *Webopedia*, 29 June 2010, <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.
- Beowulf, 'Cyber Threat to Pentagon is Global: China, Russia Near Peers of US', *osint*, 1 October 2010, <http://www.mail-archive.com/osint@yahoogroups.com/msg62329.html>.
- BGPmon, *Chinese ISP hijacks the internet*, 8 April 2010, <http://bgpmon.net/blog/?p=282>.
- Bikkenin R., 'Information Conflict in the Military Sphere: Basic Elements and Concepts', *Morskoj Sbornik*, no. 10, 2003 (translated in Highbeam).
- Blakely, Rhys et al., 'Cybergang Raises Fear of New Crime Wave', *The Times*, 10 November 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece.
- Bloomfield, Adrian, 'Estonia calls for NATO cyber terrorism strategy', *The Telegraph*, 18 May 2007, <http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html>.
- Borsook, Paulina, 'How Anarchy Works – On Location with the Masters of the Metaverse, the Internet Engineering Task Force', *Wired*, October 1995, <http://www.wired.com/wired/archive/3.10/ietf.html>.
- Broad, William J. et al., 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 January 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?ref=johnmarkoff>.

BSI, *Taking advantage of opportunities – avoiding risks*,

https://www.bsi.bund.de/cln_165/EN/TheBSI/AboutBSI/aboutbsi_node.html;jsessionid=44577CA316658235C4799B2E891309F6.

Canwest News Service, *Great Firewall China's answer to borderless Internet*, 13 January 2007,

<http://www.canada.com/topics/news/world/story.html?id=45f6e905-5aab-4af4-8736-cf59a24b664b&k=70987>.

Carr, Jeffrey, 'Stuxnet's Finnish-Chinese Connection', *Forbes*, 14 December 2010,

<http://blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/>.

-----, *Inside Cyber Warfare. Mapping the Cyber Underworld*, Beijing et al., O'Reilly Media Inc., 2010.

CCD CoE *Proceedings of the NATO CCD COE Conference on Cyber Conflict*, Tallinn July 15-18 2010,

<http://www.ccdcoe.org/conference2010/>.

-----, *Joint Workshop on Countering Botnets*, 4 January 2011, <http://www.ccdcoe.org/221.html>.

Chabrow, Eric, 'DHS, DoD to Tackle Jointly Cyber Defence', *Government Information Security*, 14 October

2010, http://www.govinfosecurity.com/articles.php?art_id=3010.

Cheek, Michael W., 'What is Cyber War Anyway? A Conversation with Jeff Carr, Author of "Inside Cyber Warfare"', *The new new Internet – The Cyber Frontier*, 2 March 2010,

<http://www.thenewnewinternet.com/2010/03/02/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>.

Claburn, Thomas, 'Fannie Mae Contractor Indicted for Logic Bomb', *InformationWeek*, 29 January 2009,

<http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=212903521>.

Clarke, Richard and Knake, Robert K., *Cyber War: The Next Threat to National Security and What to Do about it*, New York, HarperCollins Publishers, 2010.

Clausewitz, Carl von, *On War*, London, Penguin Books, 1982 [1832].

Coalson, Robert, 'Behind The Estonia Cyberattacks', *Radio Free Europe/Radio Liberty*, 6 March 2009,

http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html.

Commission on Critical Infrastructure Protection, *Toward Deterrence in the Cyber Dimension*, 1997,

http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf

Corbin, Kenneth, 'Obama's Cyber Chief Touts 'Resilient' Security Strategy', *eSecurity Planet*, 12 April 2011,

<http://www.esecurityplanet.com/news/article.php/3892116/Obamas-Cyber-Chief-Touts-Resilient-Security-Strategy.htm>.

Council of the European Union, *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*, 14781/1/05, 24 November 2005,

<http://register.consilium.eu.int/pdf/en/05/st14/st14781-re01.en05.pdf>.

-----, *Council Conclusions on cooperation to combat terrorist use of the Internet ('Check the Web')*,

8457/3/07, 29 May 2007, <http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf>.

-----, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, 2 December 2009,

<http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf>.

- , *Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime*, 5957/2/10, 25 March 2010, <http://www.statewatch.org/news/2010/mar/eu-council-revised-cyber-crime-conclussions-5957-rev2-10.pdf>.
- , *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime*, 15569/08, 26 April 2010, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf.
- Daily Herald, *Information Warfare*, 20 August 2001, <http://www.b66.info/InformationWarfare.htm>.
- Dancho, Danchev, 'Coordinated Russia vs Georgia cyber attack in progress', *ZDNet*, 11 August 2008, <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>.
- Defence Update, *SUTER V. Cyberworld's Black Knights*, http://defence-update.com/features/2008/may08/suter_v.htm.
- Demchak, Chris, 'Strategies for a Cyber-ed', *World Atlantic Council*, 12 August 2010, <http://www.acus.org/publication/strategies-cybered-world>.
- , 'Cybered Conflict vs. Cyber War', *Atlantic Council*, 20 October 2010, http://www.acus.org/new_atlanticist/cybered-conflict-vs-cyber-war.
- Doyle, Eric, 'RSA: Cyber War Mass Hysteria Is Hindering Security', *eWeekEurope*, 17 February 2011, <http://www.eweekurope.co.uk/news/rsa-cyber-war-mass-hysteria-is-hindering-security-21276>.
- Drew, Christopher and Markoff, John, 'Cyberwar, Contractors Vie for Plum Work, Hacking for U.S.', *The New York Times*, 31 May 2009, <http://www.nytimes.com/2009/05/31/us/31cyber.html>.
- ENISA, *Stock tacking report*, 19 September 2008, <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report>.
- Espiner, Tom, 'How Estonia's Attacks Shook the World', *ZDNet*, 2 May 2008, <http://www.zdnet.com.au/insight/security/soa/How-Estonia-s-attacks-shook-the-world/0,139023764,339288625-3,00.htm>.
- Estonian Ministry of Defence, *Cyber Security Strategy 2008-2013*, http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.
- European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection*, COM (2005) 576 final, 17 November 2005, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.
- , *Towards a general policy on the fight against cyber crime*, COM (2007) 267 final, 22 May 2007, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>.
- , *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM (2009) 149 final, 30 March 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.
- , *Regulatory framework for electronic communications in the European Union*, December 2009, http://ec.europa.eu/information_society/policy/ecom/doc/library/regframeforec_dec2009.pdf.
- , *A Digital Agenda for Europe*, COM (2010) 245 final/2, 26 August 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>.

- , *Concerning the European Network and Information Security Agency (ENISA)*, COM (2010) 521 final, 30 September 2010, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282010%290521_/com_com%282010%290521_en.pdf
- , *Cybercrime*, September 2010, http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm#part_2.
- European Council, *Report on Implementation of the European Security Strategy. Providing Security in a Changing World*, S407/08, 11 December 2008, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf.
- European Parliament and Council, *Directive*, 2009/140/EC, 25 November 2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>.
- Farwell, James P. and Rohozinski, Rafal, 'Stuxnet and the Future of Cyber War', *Survival*, vol. 53(1), 2011, pp. 23-40.
- Foucault, Michel, *Society must be defended*, New York, Pan Books Limited, 2003 [1975-6].
- Garamone, Jim, 'Lynn: NATO must get ahead of Cyber Threat', *American Forces Press Service*, 25 January 2011, <http://www.defence.gov/news/newsarticle.aspx?id=62572>.
- Gasparre, Richard B., 'The Israeli 'E-tack' on Syria – Part I', *airforce-technology.com*, 11 March 2011, <http://www.airforce-technology.com/features/feature1625>.
- GCN, *Cybersecurity: U.S. Must Craft Cyberwarfare Battle Strategy*, 18 February 2008, <http://www.gcn.com/Articles/2009/02/18/Black-Hat-Federal-Kurtz.aspx?Page=2>.
- Gibson, William, *Neuromancer*, New York, Ace Books, 1984.
- Glanz, James and Markoff, John, 'Vast Hacking by a China Fearful of the Web', *New York Times*, 4 December 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=2.
- Gorman, Siobhan, 'Hathaway to Head Cybersecurity Post', *The Wallstreet Journal*, 8 February 2009, <http://online.wsj.com/article/SB123412824916961127.html>.
- Hale, Julian, 'NATO Official: Cyber Attack Systems Proliferating', *DefenceNews*, 23 March 2010, <http://www.defencenews.com/story.php?i=4550692>.
- , 'New EDA Chief Exec Looking to Show Agency's Added Value', *DefenceNews*, 11. January 2011, <http://www.defencenews.com/story.php?i=5427857>.
- Harper, Mitchell, 'SQL Injection Attacks – Are You Safe?', *sitepoint*, 17 June 2002, <http://articles.sitepoint.com/article/sql-injection-attacks-safe>.
- Hayden, Michael, *Comments at the Georgetown University Conference on International Engagement in Cyberspace*, 29 March 2011, <http://lsgs.georgetown.edu/programs/CyberProject/InternationalEngagement/>.
- Heickerhö, Roland, 'Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations', *Swedish Defence Research Agency*, March 2010, <http://www2.foi.se/rapp/foir2970.pdf>.
- ICANN, *Bylaws*, 25 January 2011, <http://www.icann.org/en/general/bylaws.htm>.

- INFRAGARD, *The Russian Business Network: Attacking Georgia and Stealing from Americans*, 11 March 2009, http://www.nationalstrategies.com/pdf/publicSafety_GovSec_RussianBusinessNetwork.pdf.
- Institute for Security Studies, *Cybersecurity: what role for CFSP?*, 4 February 2009, [http://www.iss.europa.eu/nc/seminars/seminar/select_category/26/article/cyber-security-what-role-for-cfspbrbrussels-4-february-2009/?tx_ttnews\[pS\]=1230764400&tx_ttnews\[pL\]=31535999&tx_ttnews\[arc\]=1&cHash=206cccab0a](http://www.iss.europa.eu/nc/seminars/seminar/select_category/26/article/cyber-security-what-role-for-cfspbrbrussels-4-february-2009/?tx_ttnews[pS]=1230764400&tx_ttnews[pL]=31535999&tx_ttnews[arc]=1&cHash=206cccab0a).
- Internet Law and Policy Forum, 'A Bibliography of Internet Self-Regulation', undated, http://www.ilpf.org/events/selfreg/bib4_18.htm.
- Internet World Stats, *China Internet Usage Stats and Population Report*, 2010, <http://www.internetworldstats.com/asia/cn.htm>.
- ITU, 'Resolution 69 – Non-discriminatory access and use of Internet resources', *World Telecommunication Standardization Assembly*, Johannesburg 21-30 October 2008, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.69-2008-PDF-E.pdf.
- Jackson, William, 'How can we be at cyberwar if we don't know what it is?', *Washington Technology*, 22 March 2010, <http://washingtontechnology.com/articles/2010/03/22/cybereye-cyberwar-debate.aspx>.
- Jellenc, Eli and Zenz, Kimberly, 'Global Threat Research Report: Russia', *An iDefence Security Report*, 10 January 2007, <http://www.verisign.com/static/042139.pdf>.
- Joint Publication (JP) 3-13, *Information Operations*, 2006, http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
- Kanwal, Gurmeet, 'China's Emerging Cyber War Doctrine', *Journal of Defence Studies*, vol. 3(3), July 2009, pp. 14-22, http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf.
- Kay, David, 'As the worm turns', *The National Interest*, 1 October 2010, <http://nationalinterest.org/commentary/the-worm-turns-4168>.
- Kirk, Jeremy, Probe into US, South Korea cyberattacks stretches around the globe, *ComputerworldUK*, 15 July 2009, <http://www.computerworlduk.com/news/security/15724/probe-into-us-south-korea-cyberattacks-stretches-around-the-globe/>.
- , '5 Indicted in Long-running Cybercrime Operation', *csoonline*, 2 September 2009, http://www.csoonline.com/article/501180/5_Indicted_in_Long_running_Cybercrime_Operation.
- Klimburg, Alexander, 'Mobilising Cyber Power', *Survival*, vol. 53(1), 2011(a), p. 41-60.
- , *Ruling the Domain – (Self) Regulation and the Security of the Internet*, 2011(b), www.oiiip.at (unpublished).
- Kramer, Franklin D., 'Cyber Conflict: Challenging the Future. Speech at the Black Hat Conference 18 January 2011', *Atlantic Council*, 19 January 2011, <http://www.acus.org/news/franklin-kramer-us-should-aim-cyber-resilience>.
- Krebs, Brian, 'Following the Money: Rogue Anti-virus Software', *The Washington Post*, 31 July 2009, http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html
- Kuehl, Dan, 'From Cyberspace to Cyberpower: Defining the Problem', in Kramer, Franklin D. et al. (ed.), *Cyber power and National Security* Washington, D.C., National Defence UP, 2009.

- Lam, Willy, 'Beijing beefs up cyber-warfare capacity', *Asia Times Online*, 9 February 2010, <http://www.atimes.com/atimes/China/LB09Ad01.html>.
- Leigh, Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power*, Washington D.C., Brassey's, Inc., 2004.
- Leyden, John, 'Cybercrime 'More Lucrative' than Drugs. At least phishing fraudsters don't have Uzis', *The Register*, 29 November 2005, <http://www.theregister.co.uk/2005/11/29/cybercrime/>.
- Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare: China's master plan to destroy America*, Panama City, Pan American Publishing Company, 2002.
- Libicki, Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, Rand Corporation, 2009. http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
- Liu, Melinda, 'Blog the Record Straight', *Newsweek*, 28 February 2009, <http://www.newsweek.com/id/186996>.
- Lobban, Ian, 'Speech at the IISS', *GCHQ*, http://www.gchq.gov.uk/press/cyber_iiss.html.
- Lynn III, William J., 'Remarks on Cyber at the Council on Foreign Relations', *Crossroads*, 30 September 2010, <http://blog.cybersecuritylaw.us/2010/10/dep-def-sec-lynn-cyber-war-extends-conflict-93010.html>.
- MacKinnon, Rebecca, 'China Tightens Internet Controls in the Name of Fighting Porn, Piracy, and Cybercrime', *RConversation*, 14 December 2009, <http://rconversation.blogs.com/rconversation/2009/12/china-tightens-internet-controls-all-in-the-name-of-fighting-porn-piracy-and-cybercrime.html>.
- McMillan, Robert, 'Spanish Police shut down 'world's largest' botnet', *Techworld*, 3 March 2010, <http://news.techworld.com/security/3214049/spanish-police-shut-down-worlds-largest-botnet/>.
- Mills, Elinor, 'Study: Cybercrime Cost Firms \$1 Trillion Globally', *cnet news*, 28 January 2009, http://news.cnet.com/8301-1009_3-10152246-83.html.
- Minnick, Wendell, 'Is Beijing Behind Cyberattacks on the Pentagon?', *DefenceNews*, 2 June 2008, <http://www.defencenews.com/story.php?i=3576373&c=FEA&s=SPE>.
- Molchanov, N.A., 'Information Resources of Foreign States as a Threat to Russia's Military Security', *HighBeam*, 1 October 2008, <http://www.highbeam.com/doc/1G1-194154588.html>.
- Mudge, Raphael S. and Lingley, Scott, 'Cyber And Air Joint Effects Demonstration (CAAJED)', *Air Force Research Laboratory Information Directorate*, March 2008, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA481288>.
- Mueller, Milton, 'Dancing the Quango: ICANN and the Privatization of International Governance', *Conference on New Technologies and International Governance*, 11-12 February 2002, <http://faculty.ischool.syr.edu/mueller/quango.pdf>.
- Myrdal, Sara and Rhinard, Mark, *The European Union's Solidarity Clause. An Analysis of Article 222 of the Treaty on the Functioning of the European Union*, Swedish Institute of International Affairs, 2010, <http://www.ui.se/upl/files/44241.pdf>.
- National Security Presidential Directive/NSDP 54, *Cyber Security and Monitoring*.
- NATO, *NATO opens new centre of excellence on cyber defence*, 14 May 2008, <http://www.nato.int/docu/update/2008/05-may/e0514a.html>.

- , *Active Engagement, Modern Defence*, 19 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68580.htm.
- , *Lisbon Summit Declaration*, 20 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm?selectedLocale=en.
- , *Developing NATO's cyber defence policy*, 25 January 2011, http://www.nato.int/cps/en/natolive/news_70049.htm.
- Newsweek, *The (Evil) Cyber Empire. Inside the world of Russian hackers*, 30 December 2009, <http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html>.
- New, William, 'Controversy Over Internet governance: ITU Families And ICANN Cosmetics?', *ITU*, http://www.itu.int/osg/csd/intgov/ituinpress/new_william.html.
- Nye, Joseph S., 'Cyber Power', *Harvard Kennedy School*, May 2010, <http://belfercentre.ksg.harvard.edu/files/cyber-power.pdf>.
- OSCE Press Release, *OSCE can play important role in cyber security, says Estonian Defence Minister*, 4 June 2008, <http://www.osce.org/fsc/49775>.
- OECD, *Development of Policies for Protection of Critical Information Infrastructures. Ministerial Background Report (DSTI/ICCP/REG(2007)29/FINAL)*, 17-18 June 2008, <http://www.oecd.org/dataoecd/25/10/40761118.pdf>.
- O'Neill, Don, 'Maturity Framework for Assuring Resiliency Under Stress', *Build Security In*, 11 July 2007, <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/1016-BSI.html>.
- Open Source Center, *OSC Report: Russia – Russia Cyber Focus*, 7 May 2010, Issue, <http://publicintelligence.info/OSC-RussiaCyberFocus9.pdf>.
- Panda Security, *One-Third of All Malware was Created in the First 10 Months of 2010*, 24 November 2010, <http://press.pandasecurity.com/usa/news/one-third-of-all-malware-was-created-in-the-first-10-months-of-2010/>.
- Présidence de la République, *The French White Paper on defence and national security*, http://www.ambafrance-ca.org/IMG/pdf/Livre_blan_Press_kit_english_version.pdf.
- Presidential Decision Directive/PDD-63, *Critical Infrastructure Protection*, <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.
- Priest, Dana and Arkin, William M., 'A Hidden World, Growing Beyond Control', *Washington Post*, 19 July 2010, <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>.
- Project Grey Goose, *Phase I Report: Russia/Georgia Cyber War – Findings and Analysis*, 17 October 2008, <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.
- , *Phase II Report: The evolving state of cyber warfare*, 20 March 2009, <http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>.
- Rainsford, Sarah, 'Inside the Mind of a Russian Hacker', *BBC News*, 11 March 2010, <http://news.bbc.co.uk/2/hi/8561910.stm>.
- Rapid Press Release, *European Commission welcomes US move to more independent, accountable, international Internet governance*, 30 September 2009, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1397>.

- Reed, Thomas C., *At the Abyss: An Insider's History of the Cold War*, New York, Presidio Press, 2004, p. 269.
- Russian Federation Military Policy in the Area of International Information Security, 'Regional Aspect', *Military Thought*, vol. 16(1), January 2007.
- Sachoff, Mike, 'Chinese Bloggers Reach 50 Million', *WebProNews*, 7 January 2009, <http://www.webpronews.com/topnews/2009/01/07/chinese-bloggers-reach-50-million>.
- Sawer, Patrick, 'Top Chinese officials ordered attack on Google, Wikileaks cables claim', *The Telegraph*, 4 December 2010, <http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html>.
- Schmid, Alex P. and Jongman, Albert J., *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, & literature*, New Brunswick and New Jersey, Transaction Publishers, 2005.
- Schneider, Bruce, *The Threat of Cyberwar Has Been Grossly Exaggerated*, http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.
- Schneider, Deborah, 'Cyber Security Keynote Address for the U.S. Department of State', *United States Mission to the OSCE*, 9 June 2010, <http://www.osce.org/fsc/68524>.
- Shah, Anup, *World Military Spending*, 7 July 2007, <http://www.globalissues.org/article/75/world-military-spending>.
- Shiels, Maggie, 'Cyber war threat exaggerated claims security expert', *BBC News*, 16 February 2011, <http://www.bbc.co.uk/news/technology-12473809>.
- Simón, Luis, 'Command and Control? Planning for EU military operations', *EUISS Occasional Paper*, no. 81, January 2010, http://www.iss.europa.eu/uploads/media/Planning_for_EU_military_operations.pdf.
- Sommer, Peter and Brown, Ian, *OECD/IFP Project on Future Global Shocks: Reducing Systemic Cybersecurity Risk*, 14 January 2011, <http://www.oecd.org/dataoecd/57/44/46889922.pdf>.
- SPAMfighter News, *Botnets Help Cyber Criminals Earn Huge Revenues, says Kaspersky*, 8 August 2009, <http://www.spamfighter.com/News-12870-Botnets-Help-Cyber-Criminals-Earn-Huge-Revenues-says-Kaspersky.htm>.
- Stohl, Michael, 'Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?', *Crime, Law and Social Change*, 46(4-5), 2007, pp. 223-38.
- The Economist, *A Walk on the Dark Side*; *Economist*, 30 August 2007, http://www.economist.com/displaystory.cfm?story_id=9723768.
- , *A cyber-missile aimed at Iran?*, 24 September 2010, http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.
- Thomas, Timothy L., 'Comparing US, Russian, And Chinese Information Operations Concepts', *Foreign Military Studies Office*, February 2004, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf.
- Thompson, Mark, 'U.S. Cyberwar Strategy: The Pentagon plans to Attack', *Time*, 2 February 2010, <http://www.time.com/time/nation/article/0,8599,1957679,00.html>.
- Thornburg, Nathan, 'Inside the Chinese Hack Attack', *Time*, 25 August 2005, <http://www.time.com/time/nation/article/0,8599,1098371,00.html>.

- UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world*, March 2008, http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.
- UK Government, *A Strong Britain in an Age of Uncertainty. The National Security Strategy (UK-NSS)*, October 2010, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.
- UNGA, *Combating the Criminal Misuse of Information Technology*, A/RES/26/121, 23 January 2002.
- , *Creation of a Global Culture of Cybersecurity*, A/RES/57/239, 31 January 2003.
- , *Developments in the field of information and telecommunications in the context of international security*, A/64/386, 2 July 2007.
- , *Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/94, 24 June 2010.
- US Army TRADOC, *Cyber Operations and Cyber Terrorism*, 15 August 2005, <http://www.scribd.com/doc/2514092/Army-TRADOC-G2-Handbook-No-1-02-Cyber-Operations-and-Cyber-Terrorism>.
- US-China Economic and Security Review Commission, *China's Propaganda and Influence Operations, its Intelligence Activities that Target the United States and the Resulting Impacts on U.S. National Security*, 30 April 2009, http://www.uscc.gov/hearings/2009hearings/transcripts/09_04_30_trans/09_04_30_trans.pdf
- US Cyber Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign Against Georgia in August 2008*, August 2009, <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.
- Vaughan-Nichols, Steven J., 'How to crash the internet', *ZDNnet*, 13 February 2011, <http://www.zdnet.com/blog/networking/how-to-crash-the-internet/680>.
- Verneti, Gianmaria, 'The Power of Networking: An Insight on the Russian Business Network', *Bright*, 1 July 2010, http://flarenetwork.org/report/enquiries/article/the_power_of_networking_an_insight_on_the_russian_business_network.htm.
- Vogl, Toby, 'Malmström seeks EU powers to tackle transnational crime', *EuropeanVoice.com*, 11 November 2010, <http://www.europeanvoice.com/article/imported/malmstrvm-seeks-eu-powers-to-tackle-transnational-crime/69374.aspx>.
- Walker, Shaun, 'Was Russian Secret Service Behind Leak of Climate Change Emails?', *The Independent*, 7 December 2009, <http://www.independent.co.uk/news/world/europe/was-russian-secret-service-behind-leak-of-climatechange-emails-1835502.html>.
- Walton, Timothy, *Treble Spyglass, Treble Spear*, <http://www.c4ads.org/files/Three%20Warfare%202010.pdf>.
- Warren, Peter, 'Hunt for Russia's Web Criminals', *Guardian*, 15 November 2007, <http://www.guardian.co.uk/technology/2007/nov/15/news.crime>.
- Weir, Fred, 'Russia to drop Microsoft in quest for 'national' operating system', *The Christian Science Monitor*, 29 October 2010, <http://www.csmonitor.com/World/Europe/2010/1029/Russia-to-drop-Microsoft-in-quest-for-national-operating-system>.

WGIG, 'Report of the Working Group on Internet Governance', *Château de Bossey*, June 2005, p. 4,
<http://www.wgig.org/docs/WGIGREPORT.pdf>.

Wiener, Norbert, *Cybernetics or Control and communication in the animal and the machine*, New York, John Wiley, 1948.

Winkler, Ira, 'Guard against Titan Rain hackers', *Computer World*, 20 October 2005,
http://www.computerworld.com/s/article/105585/Guard_against_Titan_Rain_hackers.

Zeenews, *US, China, Russia have 'Cyber weapons': McAfee*, 18 November 2009,
<http://www.zeenews.com/news579965.html>.

Zhou, Ye, 'Jiefangjun Zixunhua budui jinnian chengjun' (PLA Cyberwarfare units deployed this year), *Zhongguo Shibao*, March 15 2003, <http://news.chinatime.com>.

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Foreign Affairs
- Human Rights
- Security and Defence
- Development
- International Trade

Documents

Visit the European Parliament website: <http://www.europarl.europa.eu/studies>

