# Cyber Warfare:
# Critical Perspectives

Ministerie van Defensie

# NL ARMS

## Netherlands Annual Review of Military Studies 2012

# Cyber Warfare: Critical Perspectives

Paul Ducheine, Frans Osinga, Joseph Soeters (eds.)

The Faculty of Military Sciences is part of the Netherlands Defence Academy.
This publication contributes to the faculty's academic Research Plan.

The views expressed in this publication are those of the authors and do not necessarily reflect the views of the Minister of Defence.

Word cloud: Jelle van Haaster
Cover and lay-out: Oasis Productions
Printed by: Wõhrmann Print Service

ISBN: 978 90 6704 341 0
NUR: 828

www.asserpress.nl

# Foreword

It is an excellent tradition of the Faculty of Military Sciences of the Netherlands Defence Academy to publish the Netherlands Annual Review of Military Studies. NL ARMS shows the state of affairs of scientific research in military sciences and, moreover, the extent to which researchers of the Academy contribute to this corpus of knowledge. This year researchers of the Faculty of Military Sciences focus on current research in the cyber domain.

The Netherlands Ministry of Defence has, in line with other Dutch ministries, formulated a policy to intensify activities in the realm of cyber security and cyber warfare. It is the intention of the Ministry of Defence to dedicate in the coming years, and to an increasing extent, means to address issues of the cyber security of systems, and the role of cyber in warfare (both cyber warfare itself and the role of cyber in kinetic warfare).

In line with this policy the Faculty of Military Sciences is formulating a multidisciplinary research program in this field in order to scientifically support these efforts, of course in cooperation with other research institutes. This new research program will, in any case, entail research efforts in the field of legal and operational aspects of cyber warfare, but will also combine technical and non-technical aspects of cyber warfare.

The current issue of NL ARMS comprises the building blocks of this new research program. One finds in this publication reports of research activities of staff of the Faculty of Military Sciences related to aspects of cyber security and warfare.

Wouter van Rossum

*Dean of the Faculty of Military Sciences*
*Netherlands Defence Academy*

# Table of Contents

TWO

# Cyber Security and Policy Responses

*Hans Bouwmeester, Hans Folmer & Paul Ducheine*

*Contents*

## 1. Introduction

With the adoption of the 2010 Strategic Concept, NATO member states have institutionally accepted the risk of cyber attacks as a high priority security concern. Whether based on solid facts or an acute manifestation perhaps of the risk-society we live in,[1] by developing policies and capabilities, these nations are not mere responders to the cyber environment, but are active agents that co-create the very reality they actually fear. By introducing cyber security and using terms like cyber threats, cyber attacks and cyber warfare, the cyber environment has thus been heavily militarised. In this chapter we explore how a number of nations have constructed perspectives on the cyber threat and developed – generic and military – strategies and policies to deal with that threat. In addition, we aim to de-

[1] Coker 2009.

*P. Ducheine, F. Osinga and J. Soeters (eds.), Cyber Warfare: Critical Perspectives*

scribe how states intend to apply cyberspace as a source or an instrument of power.

Our purpose is to describe how a number of states (and one major international organisation) coped with, or intend to manage cyber security. On the one hand, attention will be paid to the state of development amongst partners and allies. On the other hand, other stakeholders such as opponents and potential (ad hoc) partners will be covered. To the extent possible, a general policy description, succeeded by a separate military overview will be provided.

It will be absolutely clear that we can't be anything but incomplete in providing an overview of policy responses. For practical reasons, the analysis is therefore limited to states and one organisation of interest to the Netherlands. This involves various European and international partners (NATO, the United States, the United Kingdom, Germany, and France), as well as four (other) stakeholders originating from the various continents: China, the Russian Federation, Australia, and South-Africa. The selection of the states involved may seem random, which, on the one hand, hampers a coherent oversights of state responses. However, on the other hand, the allies selected represent some of the Netherlands' closest partners in modern security operations and possible future cyber operations as well. Besides allies, the other stakeholders also comprise (some) major regional (or global) powers.

Any description of cyber policy responses is furthermore hampered for a number of other reasons. First of all, there are the diverging views on definitions and terminology. One may easily find terms as 'computer network exploitation', 'cyber exploits operations', 'information operations', as well as 'electronic warfare' and 'information war' alongside each other. Moreover, analysis is also troubled since not all cyber policies are made public or accessible. Finally, some states have expressed mere intentions that have not materialised yet, whilst others are already 'fully operational'.

This chapter will start with a brief analysis of the Netherlands' cyber policy considerations. Secondly, policy responses from selected permanent allies will be presented, starting with NATO. Thirdly, other stakeholders, including potential (*ad hoc*) allies or opponents will be covered. Finally, conclusions will be presented.

## 2. Cyber Security in the Netherlands

The Dutch Government has issued a National Cyber Security Strategy in February 2011.[2] In this strategy it is clear that a free and safe use of the digital domain is essential to the community. Cyber security is an individual responsibility; however, cooperation amongst public and private entities is needed and encouraged. Within the government the Minister of Security and Justice has a coordinating role. The established National Cyber Security Centre is tasked to coordinate the exchange of information regarding cyber threats and security solutions amongst private and public partners.[3] It also hosts the national Computer Emergency Response Team (CERT).[4]

The Netherlands Armed Forces have no responsibility in securing the networks of other public or private industry or agencies. Nor is it their responsibility to fight cyber crime. The safety of the ICT-infrastructure in the Netherlands is a responsibility of the owner and the operator of the networks and systems. However, in case of an emergency and upon request the Netherlands Ministry of Defence (MoD) can contribute with its cyber capacity to support civil authorities.

The Netherlands Armed Forces view cyber as an operational capability that requires further development. To ensure its capabilities, the MoD is determined to enhance its digital capabilities in the coming years. That implies improving defensive capabilities, increasing intelligence and developing offensive capabilities.

The use of ICT systems has increased tremendously over the last two decades. This has helped armed forces all over the world to improve their decision cycles. Following classic military theory a war is won when our own decision cycle is faster than the adversary's. Therefore, armed forces rely heavily on ICT systems. These systems can be found in the obvious networks, e.g. communication and sensor systems, but also in all weapon systems, such as the height meter of a fighter plane or the engine management of a frigate. All depend on ICT.

It is essential that information is available and reliable at all times. This dependence on ICT makes modern forces increasingly vulnerable in a time where hackers do everything to break into our computer systems. A hack-

[2] *Parliamentary Papers* [Kamerstukken] II, 2010/11, 26 643, No. 174.

[3] The National Cyber Security Centre (NCSC) bundles knowledge and expertise (2 January 2012), <www.ncsc.nl/english/current-topics/news/the-national-cyber-security-centre-ncsc-bundles-knowledge-and-expertise.html> (Accessed 2 January 2012).

[4] See also Ch. 5 in this volume (Ducheine et al.).

er can be everyone ranging from the 16 year old kid next door to a state sponsored professional.

However, if our systems are vulnerable, this applies to the systems of our potential opponents as well. It does not matter whether the opponent is as technological developed as the Dutch forces or is an insurgent, who merely uses his mobile phone and internet. In the view of the Netherlands Armed Forces, this vulnerability needs to be exploited, as this may assist to increase its intelligence posture and to execute offensive operations.

The current activities of the Netherlands Armed Forces include the establishment of a Defence Cyber Command (DCC) and a Defence Cyber Expertise Centre (DCEC).[5]

The DCC will act as the coordinating authority for all cyber activities of the various units involved. Similar to national arrangements, the owner and the operator of networks, weapon platforms and sensor systems in the MoD will be responsible for the security. The current Defence CERT (DefCERT) will be reinforced with priority.[6] DefCERT cooperates with the national CERT and various international CERTs. Another priority is to improve the intelligence capacity. This is primarily a responsibility of the Military Intelligence and Security Service (MIVD).

The DCEC will be the armed forces' shared cyber knowledge environment. This unit will collect and disseminate knowledge on cyber.[7] It will have research and development capacity, and it will cooperate with universities and research institutes. It will have a large cyber laboratory and a test facility. Furthermore, it will provide guidelines on education, training and exercises; not only for cyber specialists, but for all military personnel. It is important to make everybody cyber aware, just as everybody is aware of the dangers of espionage.

As stated before, the Netherlands aims to develop significant operational cyber capabilities. Cyber will be treated as the fifth domain of warfare, next to land, air, sea and space. In theory, it is possible to operate in cyberspace without using the other domains, but it is very unlikely that a pure cyber conflict – a war only in the cyber domain – will take place. Possessing operational cyber capabilities will provide an advantage for future conflicts in any domain. Cyber should be seen as a force multiplier. The army – designated as the single service manager – will have an execut-

[5] *Parliamentary Papers* II, 2010/11, 32 733, No. 1, p. 19: 'Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld', 8 April 2011.

[6] *Parliamentary Papers* II, 2010/11, 26 643, No. 174, annex (NCSS).

[7] *Parliamentary Papers* II, 2010/11, 32 733, No. 1, p. 19: 'Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld', 8 April 2011.

ing role when it comes to the use of cyber. Currently the Netherlands' Armed Forces are in the process of developing a Defence Cyber Strategy and a Defence Cyber Doctrine. These documents should provide details on how cyber is to be used in military operations; how it is integrated in the operational planning process; and under which circumstances cyber will be launched. Cyber will be a new instrument in the toolbox of the military commander, one among the other means he can use to achieve his intended effects. Cyber is not something special, it is just something new.

The Dutch ambitions can only be achieved by creating and improving cyber capabilities in a coherent way, being the result of a balanced development process of personnel, technology and governance. Personnel are the most valuable factor. They need to be aware of the threats posed by, and the opportunities offered by cyber, but they also need to be educated and skilled. If the Dutch Armed Forces are to achieve their ambition, every soldier needs to have – some – cyber knowledge and skills. The real cyber warriors need to be the best in their field of expertise. Of course technology is important as well: one can only play a role in the cyber domain with the newest technology and the newest tools available. Governance is the way operational cyber capabilities are organised. Because of the known and unknown effects, cyber is considered a strategic asset, but it will be used at the operational and tactical levels as well.

## 3. International Partners

### 3.1 *NATO*

The first partner to mention is not really a partner, but the alliance in which the Netherlands already participates since its foundation 63 years ago: the North Atlantic Treaty Organization (NATO). NATO has a long history of defending its territory, though its geographical region expanded over time because of nations joining the Alliance. The first NATO attention for cyber defence goes back to 2002. It was during the 2002 Prague Summit that the Heads of State within NATO placed cyber defence on the political agenda for the first time, although NATO has been protecting its communication and information architecture already for an extensive period of time. The summit marked the start of a Cyber Defence Program within NATO.[8] In short, the focus of this programme was on NATO's own static networks. During the 2006 Riga Summit the programme and the need

[8] Noshiravani 2011, p. 4.

for protection of NATO's own Communication and Information System (CIS) networks was reiterated.[9]

A series of attacks on the Estonian public and private institutions in 2007 urged further protection. The massive electronic attack was identified as a Distributed Denial of Service (DDoS) that temporarily crippled Estonia's national internet infrastructure. The official version was that the offenders were never found, but the DDoS attack quickly followed after the relocation of a highly-controversial Red Army soldier statue in Tallinn, the capitol of Estonia.[10] From NATO's perspective the attack was an historic moment, because it was the first time that a member state formally requested assistance in the defence of its digital resources. While the attack was still on-going, NATO ministers of defence met in haste to struggle with the strategic effects of the first major cyber attack on a member state of the Alliance. The series of attacks on Estonia made it crystal clear that NATO lacked a coherent cyber strategy.[11]

During the 2008 Bucharest Summit policy-makers as well as subject matter experts reviewed the Estonian lessons learned. Section 47 of the Bucharest Summit clarified that NATO was to adopt a cyber defence concept and a cyber defence policy, and that structures and authorities needed to be developed.[12] The two major deliverables of the Bucharest Summit were the establishment of the NATO Cyber Defence Management Authority (CDMA), and NATO's accreditation of the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia. The CDMA represents an effort to centralise cyber defence operational capabilities across the Alliance on the operational level. It also functions as a centralised bureau for coordinating member responses to the full spectrum of cyber attacks.

As mentioned, NATO also certified Estonia's Cooperative Cyber Defence Centre of Excellence; an initiative which started already in 2003, when Estonia – prior to its official accession to NATO – proposed the creation of such a centre. Estonia's proposals received strong support from the Alliance's Secretary-General, Jaap de Hoop Scheffer, and during the summit communiqué he announced the establishment of the centre. He also stated that NATO was ready to 'provide a capability to assist allied nations, upon request, to counter a cyber attack'.[13]

[9] NATO 2009.

[10] Tikk, Kraska and Vihul 2010, p. 33.

[11] Hughes 2009, p. 4.

[12] NATO 2008.

[13] Hughes 2009, p. 4-5.

Meanwhile, the developments in the cyberspace accumulated rapidly and NATO leaders came with new statements on cyber defence during the 2010 Lisbon Summit. The Heads of State made clear in their Strategic Concept *Active Engagement, Modern Defence* that cyber attacks are rapidly becoming an eminent threat to the Alliance. They tasked the North Atlantic Council (NAC), the most senior political governing body of NATO, to revise NATO's cyber defence concept and policy. Further, the cyber defence guidance to the NAC was to develop the Alliance's ability to prevent, detect, defend against and recover from cyber attacks, and to use NATO's planning process to enhance and coordinate national cyber defence capabilities. In addition, the NAC should bring all NATO bodies under centralised cyber protection, while integrating NATO's cyber awareness, warning and response.[14] NATO's Secretary General approved its renewed cyber defence concept in March 2011 and its cyber defence policy in June 2011. In parallel, an Action Plan was adopted, which serves as a tool to ensure the policy's timely and effective implementation. Most items should be realised in 2012 and 2013.

The focus of NATO's cyber defence concept and policy is still on the protection of NATO's own static networks and their connections and interfaces to national static networks. But that is not enough. NATO needs to decide what kinds of capabilities are required across the entire spectrum of cyber operations. While the Alliance's scope and the core business shifted from protection of its own territory to defence on a distance with operations in Bosnia, the Mediterranean, Kosovo, Iraq, Afghanistan, the Horn of Africa, and Libya, the Alliance should broaden its cyber scope as well, and put more emphasis on deployable networks and on the operational planning level. Furthermore, new ideas on the US perspectives on 'Cyber Exploits Operations (CEO)' and 'Cyber Offensive Operations (COO)' are still too sensitive to discuss within NATO, but the Alliance will have to consider them to keep up the pace of the fast developing cyberspace.

At the moment NATO is very interested in developing a standard for cyber defence burden-sharing. So far, the Alliance has always worked on a case-by-case base to disseminate costs and collective goods, and to share the burdens. During 2012 Supreme Allied Command Transformation's (SACT's) Seminar in Washington D.C., NATO's current Secretary General, Anders Fogh Rasmussen, said that the Alliance is all about burden-sharing.[15] Last year Rasmussen launched the notion of 'smart defence' and

[14] NATO 2010.

[15] NATO 2012.

this year he introduced 'connected forces'. In times of austerity, smart defence and connected forces encourage allies to cooperate in developing, acquiring and also maintaining capabilities to meet current security problems. That means an Alliance-broad sharing and pooling of capabilities, setting priorities and coordinating efforts. NATO is very eager to make that also applicable for its collective cyber defence.[16]

### 3.2 *United States*

The United States (US) is still the major Atlantic partner of the Netherlands. In May last year US President Obama signed the 25-pages *International Strategy for Cyberspace*.[17] It is a comprehensive US cyberspace strategy, centred around seven key international policy priorities that aim to foster a more open, interoperable, secure, and reliable cyberspace through engagement across government, internationally, and with the private sector. The seven policy priorities are: (1) Economy: Promoting International Standards and Innovative Open Markets, (2) Protecting Own Networks, (3) Law Enforcement: Extending Collaboration and the Rule of Law, (4) Military: Preparing for 21st Century Security Challenges, (5) Internet Governance, (6) International Development, and (7) Internet Freedom.

Though there is no overarching authority or a single department in the lead, US Secretary of State, Hillary Clinton, referred to the document as an 'integrated, whole of government approach' that articulates for the first time the principles that will guide the US government's crosscutting cyberspace-related efforts. Clinton explained that the document contains no silver bullet for US cyber challenges, but she said that a broad strategy is key to presenting a unified front on cyberspace policy, avoiding stove-piped discussions.[18] Howard Schmidt, Obama's so-called 'cyber czar', explains that five departments are involved in this international cyberspace strategy: the Departments of State, Justice, Commerce, Homeland Security and the Department of Defense (DoD). Close cooperation of these departments is one of the (desired) major outcomes of the strategy, e.g., leading to intergovernmental cyber education.[19] The Obama administration considers the strategy more as sweeping principles unifying government departments, rather than a detailed and prescriptive plan addressing the malicious eccentricities in cyberspace.

[16] NATO Allied Command Transformation 2012.

[17] President of the United States 2011.

[18] Hoover 2011.

[19] Schmidt 2011.

Domestically, the Department of Homeland Security, created in 2002, unites 22 federal entities for the common purpose of improving the US internal security. The Secretary of Homeland Security has important responsibilities regarding US cyberspace security, such as developing a comprehensive national plan for securing key resources and critical infrastructure, providing crisis management in response to an attack, and offering technical assistance to the private sector and other government institutions.[20] In November 2011, the Department released its *Blueprint for a Secure Cyber Future* based on the 2010 published *Quadrennial Homeland Security Review*. The blueprint describes two areas of action: (1) today's protection of US critical infrastructure, and (2) tomorrow's creation of a stronger cyber ecosystem. Each year the Department of Homeland Security will evaluate the progress they made in both mentioned action areas.

Militarily, in July 2011 the United States distributed the *Defense Strategy for Operating in Cyberspace* just a few months after the launch of the overarching *International Strategy for Cyberspace*. The document is also known as *Pentagon's Cyber Strategy*. Although the complete document is classified and 40 pages long, this 19 page summary explores the strategic context of cyberspace before describing five 'strategic initiatives' to set a strategic approach for the US DoD's cyber mission. The main strategic initiative is to treat cyberspace as an operational domain to organise, train, and equip so that US DoD can take full advantage of cyberspace's potential. Other initiatives include the protection of US DoD networks and systems, cooperation with other US government departments and the private sector, and international cooperation with US international partners to strengthen collective cyber security. The DoD intends to present its defence strategy as a warning to deter potential adversaries, who should consider the consequences when cyber-attacking the US 'If you shut down our power grid, maybe we will put a missile down one of your smokestacks', a US military official said in the *Wall Street Journal*.[21]

The introduction of the Pentagon's Cyber Strategy caused a lot of fuzz, and both non-Western as well as Western media – including American ones – expressed concern. The strategy sparked the debate over a range of sensitive issues the Pentagon left unaddressed, including whether the US will ever be certain about an attack's origin, and whether a computer sabotage case is serious enough to constitute an act of war. These questions have already been a topic of dispute within the military for quite a while. One

[20] Tikk 2011.

[21] Cited in: Gorman and Barnes 2011. This is in line with the *International Strategy for Cyberspace*.

idea gaining momentum at the Pentagon is the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation.[22]

The nucleus of all military cyber activities is US Cyber Command (US-CYBERCOM), which is an armed forces sub-unified command subordinate to US Strategic Command. Cyber Command is composed of several service components, and units from military services that will provide joint cyber services. The command plans, coordinates, integrates, synchronises and conducts activities to direct full spectrum military cyberspace operations to enable actions in all domains. Its mission is to ensure US freedom of action in cyberspace while denying the same to their adversaries.[23] After becoming 'initial operational capable' in May 2010, Cyber Command inspired many other nations in the cyber arena to create cyber task forces or cyber commands, such as South-Korea, Norway, the United Kingdom, and the Netherlands.

Momentarily, the US DoD is developing a *Joint Concept on Cyberspace* (JCC). The concept identifies strategic effects and broad military capabilities available to achieve 'cyberspace superiority'. Cyberspace superiority is described as 'a degree of dominance one force holds over an adversary that permits freedom of action in cyberspace at a given time and place while denying the same to that adversary'. It will be achieved through a concerted effort with the right balance and integration of advanced technology and cyber capabilities, an adequate command and control (C2) structure, clear guidance, policies and a legal framework, and last but not least a well-trained and mission-ready task force. The JCC has distinguished three different ways to gain cyberspace superiority: (1) US DoD Global Information Grid Operations (DGO) to protect positioning information, (2) Defensive Cyber Operations (DCO) to protect US DoD's own static and deployable networks, and (3) Offensive Cyber Operations (OCO). The last category includes activities to access an adversary's hardware and software by both remote and direct means; attacks on cyber embedded processors and controllers of an adversary's equipment and systems; attacks on the adversary information in order to dissuade, undermine or deceive him; mitigation and bypassing an adversary's measures to execute OCO; and to provide OCO decision-makers with accurate intelligence of the cyberspace.[24]

[22] Gorman and Barnes 2011.

[23] United States Strategic Command 2012.

[24] US Department of Defense 2011b, p. 2-3, 5, 32-35.

Showing their offensive cyber aims obviously is a part of the US battle of the narrative. Since most offensive cyber weapons – by their nature – can only be used once before the rest of the world will have an adequate answer to these weapons, the US DoD is very willing to openly share their offensive intentions without compromising in detail their tactics, techniques and procedures. The deterring strategic message in the JCC is: don't mess with us! On 19 February 2012, General Robert Kehler, the current Chief of US Strategic Command, signed the JCC, and it is now up to General Martin Dempsey, the US Chairman Joint Chiefs of Staff, to approve the document as an official USDoD concept.[25]

### 3.3 *United Kingdom*

Many developments in cyberspace occurred since the United Kingdom (UK) published its first cyber security strategy in 2009. Therefore, in November 2011, the UK published a revised edition of the strategy: *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. The strategy sets out the vision for the United Kingdom in 2015, which reads: 'Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and rule of law, enhance prosperity, national security and a strong society.'[26] Alongside emphasis on individual responsibility of cyberspace participants, ranging from private companies to everyone at home and at work, the strategy announced that the intelligence agencies together with the Ministry of Defence (MOD) will have a strong role in improving UK's understanding and reducing the vulnerabilities and threats they are facing in cyberspace. The Government Communication Headquarters (GCHQ), a British intelligence agency responsible for providing signals intelligence and information assurance to UK's government and armed forces under responsibility of the Secretary of State for Foreign and Common Wealth Affairs (although the GCHQ is no part of the Foreign Office) will play a central role in synchronising all cyber efforts. But also the MOD itself, the Home Office, the Cabinet Office (a supporting department for the Prime Minister and the Cabinet), and the Department for Business, Innovations and Skills will bolster their specific individual cyber capabilities.[27]

In 2010, the UK Government issued a Defence review, called *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review,*

[25] Ghioni 2012.

[26] UK Government 2011, p. 21.

[27] UK Government 2011, p. 25.

on the rapidly evolving security environment. The main purpose of this document was to set out the Government's determination to make the right decisions for the long term defence and prosperity of the country, although the document also functions as the foundation for forthcoming cuts in the size of the British Armed Forces.[28] Cyber security, however, assumes a prominent place in the review, and the document announced a GBP 650 million funding for a new *National Cyber Security Programme*, a programme to transfer the Government's response to cyber threats, and to allocate financial resources to departments and agencies that have a key role to play. The review also introduced a new organisation, the UK Defence Cyber Operations Group, to mainstream cyber security throughout the MOD and to ensure the coherent integration of cyber activities across the spectrum of defence operations.[29]

Britain's Chief of Defence Staff, General David Richards, was convinced that the UK Armed Forces would face a cultural change. He explained his opinion in the *Online Daily Mail*:

> Whether we like it or not, cyber is going to be part of future warfare, just as tanks and aircraft are today, and it could become the dominant form. It will be cyber or banking attacks – that's how I'd conduct a war if I was running a belligerent state or a rebel movement. It's semi-anonymous, cheap and doesn't risk people.[30]

The British Armed Forces will be expanded with two new cyber units. The first unit will be a Joint Cyber Unit as part of the new UK Defence Cyber Operations Group. It will be hosted by the GCHQ at Cheltenham and its role will be to develop new tactics, techniques and plans to deliver military effects through operations in cyberspace. The unit considers the future contribution of reservists for bringing in specialist cyber knowledge and skills. The UK MOD recently opened a new Global Operations and Security Control Centre (GOSCC) at Corsham to act as a hub for the armed forces' cyber defence. A second Joint Cyber Unit embedded within this GOSCC will develop and use a range of new techniques, including proactive measures to disrupt threats to UK's information security.[31]

[28] UK Prime Minister's Office 2010.

[29] UK Government 2010, p. 47.

[30] Daily Mail 2011.

[31] UK Government 2011, p. 26-27.

Although not openly stated and documented, the cyber scope of the British Armed Forces will be on Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO), and Cyber Exploit Operations (CEO).

The UK MOD is also strengthening relations with key allies to improve their collective awareness and response to cyber threats. They use a hierarchy in their allies: their primary allies are those of the so-called five-eyes-community,[32] followed by other major NATO nations. In March 2012, US President Barack Obama and UK Prime Minister David Cameron vowed to work together to protect private and government networks from cyber attacks.[33] The two nations are also working on a Memorandum of Understanding to share potential threat information, conduct joint planning, and cooperate in the pursuit of criminals.[34]

### 3.4 *Germany*

Germany's cyber security is streamlined in its 2011 *Cyber Security Strategy for Germany.* The German Federal Government recognised that cyber security must be based on a comprehensive approach. For the next years the Federal Government will focus on ten strategic areas, which can be grouped into the following clusters: (1) Protection and security of German critical networks and systems, (2) Set up of a National Cyber Response Centre (NCRC), and a National Cyber Security Council (NCSC), (3) Effective cyber crime control, (4) International cooperation, and (5) Personnel development in federal authorities. The NCRC's main task will be to optimise operational cooperation between all German state authorities, and to improve the coordination of protection and response measures for cyber related incidents. The centre will report to the Federal Office for Information Security (*Das Bundesamt für Sicherheit in der Informationstechnik* – in Germany abbreviated as *BSI*), the German government agency in charge of managing computer and communication security for the German Federal Government. The German Federal Police, the German Federal Intel-

[32] The five eyes community: US, UK, Canada, Australia, New Zealand. The community, especially focused on military and intelligence operations, originates from The Technical Cooperation Program (TTCP) which started in 1957. The TTCP was a spin-off of the ABCA (America, Britain, Canada and Australia as members, and later New Zealand as observer) Armies Program which was established in 1947 and encouraged interoperability and standardisation of training and equipment. The ABCA Armies Program is a special relationship between (native) English speaking nations that came into being as ABDACOM (America, Britain, Dutch and Australia Command) focused on the operations in the Pacific during World War II.

[33] Factsheet: see US Embassy London 2012.

[34] UK Government 2010, p. 47.

ligence Service, the *Bundeswehr* (German Armed Forces) and authorities supervising critical infrastructure operators will closely work together in the centre within the framework of their statutory tasks and powers. The National Cyber Security Council's mission is the cooperation between the public and private sector to identify and remove structural causes to potential cyber crises. It will comprise business and federal government representatives as well as associated members. Academia will be involved, if required.[35]

The cyber security strategy mainly focuses on civilian approaches and measures. They are complemented by measures taken by the German Armed Forces to protect its capabilities and measures. There are, unfortunately, no unclassified documents of the German Armed Forces available explaining their capabilities in cyberspace. However, the German magazine *Der Spiegel,* one of Europe's largest publications of its kind with a distinctive reputation for revealing political misconduct and scandals, in 2009 published an online article stating that the German Armed Forces train their own hackers and not only to prevent Germany from a DDoS attack. Isolated from the population, in the Tomberg Barracks in Rheinbach, a picturesque small town near Bonn, a unit of almost eighty CIS specialists under command of the Head of the German Armed Forces Strategic Reconnaissance Unit, a German brigadier-general, is testing the latest methods of infiltrating, exploring, manipulating, and destroying networks. The unit, known by its innocent official name 'Department of Information and Computer Network Operations', is preparing for an electronic emergency, including digital attacks on outside servers and networks.[36]

### 3.5 *France*

In June 2008 the French Ministry of Defence issued a *White Paper on Defence and National Security (Défense et Sécurité nationale, Le Livre Blanc)* in which it emphasised the threat of large-scale cyber attacks against critical infrastructure as an important national security concern. The cyberspace is recognised as an area in which sovereignty and responsibility need to be fully expressed, and therefore the white paper developed a two-pronged strategy: on the one hand, a new concept of cyber defence, organised in depth and coordinated by a new Security of Information Agency under the purview of the General Secretariat for Defence and National Security. On the other hand, there is the establishment of an offensive cyber war capability, part of which will operate under the command of the French

[35] Bundesministerium des Innern 2011, p. 6-12.

[36] Goetz, Rosenbach and Szandar 2009.

Joint Staff, while the other part will be developed within the specialised services.[37]

Three years later, in February 2011, the Secretary General of Defence and National Security, Mr. Francis Delon, launched a new document *Stratégie de la France: Défence et sécurité des systèmes d'information* (French Strategy for the Defence and Security of Information Systems) in which he explained that the creation of the National Agency for the Security of Information Systems (*l'Agence nationale de la sécurité des systèmes d'information, ANSSI)* in 2009 was a first step in reinforcing the French national cyber defence capabilities. The ANSSI's mission contains detecting and reacting to cyber attacks, preventing cyber threats by supporting research and development, and providing information to the French government. The strategy also shows the French cyber ambitions, starting with its desire to become a global power in cyber defence. Other ambitions include a guarantee of France's information sovereignty and freedom of decision, improvement of critical infrastructure's cyber security, and maintaining privacy in cyberspace.[38]

The Center for Strategic and International Studies states in its document *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* that France is now developing an offensive cyber warfare capability. Both the army and the air force have electronic warfare units which will be prepared for Offensive Cyber Operations (OCO) and Cyber Exploit Operations (CEO). The French army has one brigade for intelligence, surveillance and reconnaissance that includes two electronic warfare regiments. The air force has one fleet for electronic warfare including a C-160G Gabriel for electronic surveillance. Offensive cyber capabilities are also being pursued by the French intelligence service.[39]

[37] Ministère de la Défense 2008, p. 12-13.

[38] Delon 2011, p. 3-14.

[39] Lewis and Timlin 2011, p. 11-12.

## 4. Other Stakeholders

### 4.1 *China*

> *To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.*[40]

Impressed by US technological and information dominance during the First Gulf War (1991) and the Kosovo War (1999), the People's Republic of China (PRC) and People's Liberation Army (PLA) doctrinal thinkers began to analyse western military victories.[41] The US success in Iraq also demonstrated the failure of Iraq's Chinese and Russian-made weapons.[42]

Since then, China has emerged as a global power in information and communications technology (ICT). China has 'crafted and implemented a multifaceted strategy by integrating its foreign, domestic, military, and economic policies in order to achieve its national objectives'.[43] Guided by a 15-year (2006-2020) development strategy, '*informatization* of Chinese civilian and military infrastructure' is a priority of the Chinese Communist Party and PRC government in order to ensure sustained economic growth, to compete worldwide in the ICT field, and to guarantee national security.[44]

To that end, China's military-industrial complex (and its constituent elements) comprises military and civilian R&D functions, enabling the PLA to 'access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development', accomplished through 'technology conferences and symposia; legitimate contracts and joint commercial ventures; partnerships with foreign firms; and joint development of specific technologies'.[45]

In July 2010, the PLA General Staff Department (GSD) unveiled the country's first 'Information Support (Assurance) Base'.[46] According to Stokes et al., the base is China's Cyber Command, tasked to deal with

[40] Mao Tse-Tung, cited in: US Army, Battlefield Deception, FM 90-2, Ch. 5, 'Deception Means', at: <www.fas.org/irp/doddir/army/fm90-2/90-2ch5.htm>.

[41] Billo and Chang 2004, p. 28.

[42] Baocun and Li Fei 1995.

[43] Billo and Chang 2004, p. 26; US Department of Defense 2003.

[44] PRC Embassy in Washington DC2006.

[45] US Department of Defense 2011a, p. 5-6.

[46] Hagestad 2012, p. 26, uses similar wording: 'Information Security Base'.

cyber threats and to safeguard China's national security.[47] The formation of the base demonstrates the importance of ICT and its role in future military development within Chinese thinking.[48]

Two main lines of thought can be deduced from Chinese reports and statements on cyber warfare.[49] First, cyber warfare strategy (as does conventional warfare strategy)[50] refers to Sun Tzu and his *Art of War* in almost every written document.[51] Moreover, it very much relies on the pillars set out in *Unrestricted Warfare*.[52] As argued by Hagestad, the pillars of *The Art of War* and *Unrestricted Warfare* have been implemented in China's Information Warfare strategy: 'The eight pillars [...] include the following mandates; omni-directionality, synchrony, limited objectives, unlimited measures, asymmetry, minimal consumption, multidimensional coordination and adjustment and control of the entire process.'[53] Second, cyber warfare strategy serves national goals because it is an efficient way of carrying out asymmetric operations against opponents.[54] Information dominance for political, economic, and military purposes necessitates control (or even superiority) of both the electromagnetic spectrum and the global cyber sphere.[55]

Diplomatically, China – frequently in line with Russia – has enlarged diplomatic efforts in multilateral and international cyber forums to promote enhanced international control over cyber activities, although China has not yet agreed (with other States) that existing legal regimes, such as the Law of Armed Conflict, may apply in cyberspace.[56]

China's 2004 White Paper on National Defence states that 'informationalization has become the key factor in enhancing the war fighting capability of the armed forces' and that the PLA takes informationalization 'as its orientation and strategic focus'.[57] According to the US DoD's annual assessment on China's military capabilities, 'developing capabilities for cyber warfare is consistent with authoritative PLA military writings'.[58]

[47] Stokes, Lin and Hsiao 2011, p. 3.

[48] Stokes, Lin and Hsiao 2011, p. 3.

[49] Billo and Chang 2004, p. 28

[50] Confirmed by Kissinger 2011, p. 22-32.

[51] See Hagestad 2012, p. 29-36.

[52] See Qiao Liang and Wang Xia 2002.

[53] Hagestad 2012, p. 30.

[54] In that line: US Department of Defense 2011a, p. 5-6.

[55] Stokes 2011, p. 3.

[56] US Department of Defense 2011a, p. 5-6.

[57] Lewis and Timlin 2011, p. 8-9.

[58] US Department of Defense 2011a, p. 5-6.

Two military doctrinal writings – *Science of Strategy* and *Science of Campaigns* – identify information warfare (IW) as vital to accomplishing information superiority and an effective means for countering a stronger rival, thereby illustrating the effectiveness of IW and computer network operations in conflicts, and advocating targeting adversary C2 and logistics networks prior to, or in the initial phases of conflict.[59] According to the *Science of Strategy* in information warfare the command and control system is the heart of information collection, control, and application on the battlefield, and forms the centre of gravity for 'targeting'.[60] Described by Krekel, Adams and Bakos: 'PLA leaders have embraced the idea that successful war fighting is predicated on the ability to exert control over an adversary's information and information systems, often pre-emptively. This goal has effectively created a new strategic and tactical high ground, occupying which has become just as important for controlling the battle space as its geographic equivalent in the physical domain.'[61] Although the Air Force is officially responsible for information operations and information counter-measures, the PLA General Staff Department's 3rd and 4th Department seem to be the key players. The 4th Department, overseeing electronic counter-measures and research institutes developing information warfare technologies, is responsible for military cyber capabilities, whereas the 3rd Department is responsible for signals intelligence and focuses on collection, analysis and exploitation of electronic information.[62] The 4th and 3rd Departments conduct advanced research on information security.[63] Apparently, the PLA seeks to 'unite the various components of IW under a single warfare commander',[64] which is demonstrated by numerous reports describing integrated and joint training within and between China's seven military regions.[65] As said, the PLA arguably hosts China's Cyber Command, integrating the various defensive and offensive elements of the state.[66] According to Hagestad, this command's mission is to address potential cyber threats and strengthen China's cyber infrastructure, as was reiterated by President Hu Jin.[67]

[59] Also: Lewis and Timlin 2011, p. 8-9; and Xinhua.net 2004.
[60] US Department of Defense 2011a, p. 5-6.
[61] Krekel, Adams and Bakos 2012, p. 8.
[62] Krekel 2009, p. 6, 31.
[63] Krekel 2009, p. 30, 32.
[64] Krekel, Adams and Bakos 2012, p. 8.
[65] Billo and Chang 2004, p. 39; Krekel 2009 and Krekel, Adams and Bakos 2012, p. 21.
[66] Hagestad 2012, p. 25.
[67] Hagestad 2012, p. 25.

As in Russia (see below), the PLA also maintains ties with universities and other organisations in the public domain,[68] civilian hackers, and state-owned enterprises[69] enabling it to expand its capabilities, with some units directly embedded in commercial firms and universities.[70]

## 4.2 *The Russian Federation*

> *The greater the technological accomplishments, the greater the vulnerability for a cyber attack.*[71]

The Russian Federation's (RF's) cyber posture was one of President Putin's highest priorities after taking office in 1999. The first *Information Security Doctrine,* prompted by analysis of experiences in the first Chechen War,[72] was issued in 2000[73] by Russia's Security Council's Department of Information Security.[74] As a result, laws have been enacted and amended to accommodate powers for governmental and non-governmental bodies in this domain, enabling the Russian government to control the critical Russian internet structures,[75] which features one of the most vivid and socially engaged internet communities around the world.[76] Consequently, the RF's current cyber strategy is said to be holistic, coherent, and robust, integrating state, academic and private cyber resources and expertise.[77] Instead of using the term 'cyber', the RF prefers the wider phenomena 'Information Security', 'Information Warfare' or 'Information Operations':[78] 'Russia views cyber-capabilities as tools of information warfare, which combines intelligence, counterintelligence, *maskirovka*, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities'.[79] Unlike the US and the UK, both taking a holistic stance by

[68] Krekel, Adams and Bakos 2012, p. 55 et seq. Also: Carr 2012, p. 172.

[69] Hagestad 2012, p. 18. Also: Oakley 2011, p. iv.

[70] Lewis and Timlin 2011, p. 8-9.

[71] Burutin, in: Carr 2012, p. 166.

[72] Goble 1999.

[73] Available on the Security Council of the Russian Federation website at <www.scrf.gov.ru/documents/6/5.html>.

[74] Carr 2012, p. 218.

[75] Carr 2012, p. 218 et seq.

[76] As a group, Russians 'are the most engaged social networking audience in the world', according to: comScore.com 2009.

[77] Carr 2012, p. 217.

[78] Giles 2011, p. 46. Cyber is used though in reference to the US and China.

[79] Mshvidobadze 2011.

referring to defensive and offensive capabilities,[80] Russia's Information Security Strategy appears to be merely defensive in nature, at least in open sources.[81]

Russia's information security (or cyber) doctrine (as does China's) appears to be – at least in part – a product of fear of US superiority in the cyber field.[82] Former President Medvedev suggested Western instigation in the Arab Spring uprisings, in that respect referring to necessary preparations for the RF in order to counter rebellion of this kind.[83] However, as Burutin's citation above illustrates, Russian's information security strategy and doctrine is the result of strategic thinking as well, exploiting opponent's vulnerabilities to the maximum extent possible. In addition, 'the devaluation of spiritual values, the propaganda of examples of mass culture which are based on the cult of violence, and on spiritual and moral values which run counter to the values accepted in Russian society', seems to be a third driving factor,[84] whereby internet is viewed by some as a threat to the Russian security as a whole.[85]

In the international arena, the RF is supportive of international and the UN's efforts to ensure international information security.[86] Unlike states like the US, the RF advocates emphasis on international regulation. This could be explained by the fact that Russia may be lagging behind other States.[87]

Catching up with these states on the one hand, and meanwhile trying to limit further development by those states through international binding agreements on the other hand, serves as a plausible strategic explanation. On paper, Russia is willing to contribute to international arrangements.[88] However, as disinformation and misdirection is an essential tactic in Rus-

[80] See above the sections dealing with the US and the UK.

[81] Giles 2011, p. 47.

[82] Billo and Chang 2004, p. 110, referring to the copying (by Russia and China) of US Information Operations doctrines: Major M. Botysov, 'In Foreign Navies', in the Russian Military Naval Forces publication on October 19, 1995. Also: Giles 2011, p. 48.

[83] Giles 2011, p. 49.

[84] Information Security Doctrine. See also V.L. Sheynisin Giles 2011, p. 48.

[85] According to FAPSI's First Deputy Director General Vladimir Markomenko, in Giles 2011, p. 49.

[86] Dylevsky et al. 2007; Talbot 2010.

[87] Giles 2011, p. 50; Gorman 2010.

[88] As demonstrated by the so called Shanghai Cooperation Organisation (SCO), 'on advancing common rules of conduct in the international community in the field of safeguarding international information security', in: SCO (2011); also BBC Monitoring: 'Russian pundit interviewed on US information operations conference', Rossiya TV 1950 GMT 27 April 2009.

sia's (cyber) strategy, it is difficult to determine which parts of the doctrine have actually been implemented, and which represent deception.[89] Russia's alleged support for international arrangements contrasts with its reluctance to join proposed initiatives such as the European Convention on Cybercrime. However, this position can easily be explained by the fact that Moscow is not keen on working together with foreign law enforcement officials looking into something like the 2007 cyber attacks on Estonia, and 'it surely does not want to risk exposure of its links to the thugs who run cyber crime syndicates such as the Russian Business Network (RBN)' according to Radio Free Europe.[90]

Russia's 'Comprehensive Information Protection System' as it is referred to by Jeffrey Carr, comprises numerous military and non-military bodies, including the Federal Security Service (FSB, *inter alia* the 16th Directorate), Ministry of Internal Affairs (MVD, especially 'Directorate K'), the Federal Service for Technical and Export Control (FSTEC), the Federal Security Organizations (FSO), as well as various bodies within the Russian Ministry of Defence and the Russian Armed Forces. The top structure comprises the Presidency, the RF's Security Council, and its Department of Information Security.[91]

Notwithstanding this public and governmental formal system, Russia has integrated public and 'private' resources into comprehensive *modus operandi* enabling it to initiate cyber or information operations in support of its domestic and international policy, as was demonstrated by non-military cyber attacks against (some of) its opponents (*inter alia*: Chechnya, Kyrgyzstan, Estonia, Lithuania, Georgia and Ingushetia).[92]

The Kremlin's alleged 'cyber war by proxy' modus operandi is described in Carr's *Inside Cyberwarfare – Mapping the Cyber Underworld,* and is characterised by a three-tiered model. The Kremlin apparently establishes command and control over Russian hacktivists, through various national youth associations (such as *Nashi* and *United Russia*), 'whose membership includes hackers, resulting in an organised, yet open call for unaffiliated hackers to join in', and protected by Russian criminals, whilst keeping its distance from the hackers' activities.[93] Others, however, appear far more

[89] Billo and Chang 2004, p. 108; Carr 2012, p. 169.

[90] Mshvidobadze 2011.

[91] Billo and Chang 2004, p. 115; Carr 2012, p. 221.

[92] Carr 2012, p. 161.

[93] Carr 2012, p. 119, 168.

sceptic *vis-à-vis* Russia's abilities to recruit cyber specialists in competition with commercial enterprises.[94]

The Russian Federation released its new military doctrine in February 2010. The Doctrine describes modern military conflict, featuring the integration of military and non-military capabilities; an increased role for information warfare; and early implementation of measures of information warfare 'to achieve political objectives without the use of military force'.[95] As a result, forces and means of information warfare, and 'new types of precision weapons and the development of their information security' as part of 'the information space of the Russian Federation' are required.[96] To this effect, the RF published its military Cyber Strategy in January 2012.[97]

Russia's application of cyber warfare in military campaigns, however, goes back to the days of the Second Russian-Chechen War (1997-2001).[98] Subsequently, Russia allegedly applied 'by proxy' information 'warfare' and cyber capacities, in the Estonia Cyber attacks (2007),[99] and the Russia-Georgia War (2008).[100] In the latter case, cyber was used alongside kinetic lines of operations.[101] Starting in the 1980s, Russia has been building up cyber warfare doctrine, initially focused on CNE to CNA.[102] Since then, Russia's Armed Forces, working together with IT experts and academics, have developed 'a robust cyber warfare doctrine'.[103] The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. Information weaponry, i.e. weapons based on programming code, receives paramount attention in official cyber warfare doctrine.[104]

[94] Giles 2011, p. 54-55 versus Mshvidobadze 2011.

[95] Lewis and Timlin 2011, p. 19.

[96] 'ВоеннаядоктринаРоссийскойФедерации', Russian Presidential Executive Office, 5 February 2010, <http://news.kremlin.ru/ref_notes/461>.

[97] See (Russian only): <www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>, for a partial translation: see <www.aofs.org/2012/04/15/russia%C2%B4s-cyber-strategy-published/> (Accessed 9 May 2012).

[98] Carr 2012, p. 3.

[99] Tikk, Kraska and Vihul 2010, p. 33.

[100] Tikk, Kraska and Vihul 2010, p. 89; Carr 2012, p. 15 and 106 et seq.; also: A(natoly) Tsyganok, 'Informational Warfare – a Geopolitical Reality', in: <rbth.ru/articles/2008/11/05/051108_strategic.html> (November 5, 2008) (Accessed 9 May 2012).

[101] Giles 2011, p. 46; NATO Defence College 2010.

[102] Carr 2012, p. 162, referring to Billo and Chang 2004, p. 107 et seq.

[103] Billo and Chang 2004, p. 9.

[104] Billo and Chang 2004, p. 9.

Following the first *Information Security Doctrine* (2000), Russia's military scholars and academics published numerous IO articles, such as *Non-Contract Wars*, by Major General (ret.) V.I. Slipchenko,[105] and General A. Burutin's *Wars of the Future will be Information Wars.*[106]

As described by Burutin, kinetic force 'will have to make room for information superiority', whereas future wars will shift to attacking 'state and military control systems, navigation and communication systems, and other crucial information facilities'.[107] Consequently, the use of information weapons can be used by a small specialised team, without (large-scale) physical cross-border operations taking place.[108] In general, the RF views information conflict at the various levels of command, i.e. the strategic, operational, and tactical levels.[109] Despite the holistic view on information security, Giles hints at rivalry between civil and military authorities in cyber issues.[110]

### 4.3 *Australia*

The regional power Australia is an active player in the cyber realm. Australians have been quickly to embrace the internet in their lives and business. For most of them it is now part of daily routine for communicating with friends and family, shopping, paying bills and doing business, says the Australian Attorney-General in his introduction of the 2009 Australian *Cyber Security Strategy.*[111] The strategy encompasses three major objectives. First the individual awareness of Australians for cyber risks, including steps to take for protecting their identities, privacy and finances online. Second Australian businesses need to operate secure and resilient information and communications technologies to protect the integrity of their own operations and identity and privacy of their customers. Third the Australian Government ensures its information and communication technologies are secure and resilient. The strategy also introduced two new organisations

[105] Carr 2012, p. 222.

[106] General Alexander Burutin, Deputy Chief of the General Staff, at the National Forum of Information Security (Info Forum-10), Moscow, February 2008 (see: Carr 2012, p. 165).

[107] ITAR-TASS news agency, 31 January 2008, in Giles 2011, p. 50.

[108] General Alexander Burutin, Deputy Chief of the General Staff, at the National Forum of Information Security (Info Forum-10), Moscow, February 2008 (see: Carr 2012, p. 165).

[109] Thomas 2005, p. 79-80.

[110] Giles 2011, p. 52 et seq.: D. Litovkin. 'General Staff Prepares for Cyber War', *Izvestiya*, 27 February 2009.

[111] Australian Government 2009.

that will support the strategy: CERT[112] Australia and the Cyber Security Operations Centre (CSOC).[113] CERT Australia will be the national hub within the Australian government for the provision of cyber security information and advice to the Australian community. Established as an initiative mentioned in the Cyber Security Strategy, the CSOC provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national interest and importance.[114]

It was in his 2008 published book *Australia and Cyber-warfare* that Australian retired Air Commodore Gary Waters emphasised Australia's need for defence as well as offensive cyber capabilities. In his conclusion he argues for an Australian cyber warfare centre to coordinate the operations.[115] His proposal was realised in 2009 when Australia's *Defence White Paper* was introduced. The Department of Defence announced in the white paper a major boost of the Department of Defence's cyber warfare capability. Although many of the capabilities remain classified, in sum they consist of a much-enhanced cyber situational awareness and incident response capability. The establishment of the CSOC was also announced in the white paper.[116] However, Chris Hanna remarks in his article *Cyber Operations and the 2009 Defence White Paper: Positioning the Australian Defence Organisation to Be Effective, Transparant and Lawful* that it is difficult to determine the function of either the CSOC or the wider Australian Defence Force (ADF) that flows from the white paper's discussion on cyber operations. Likewise it remains unclear whether an offensive or even a counter-attacking defence capability is envisioned by the Australians.[117] Following the release of the white paper, when questioned on the potential offensive role of the CSOC, the Australian Chief of Defence Force referred to the classification of the information, while the Secretary of Defence reiterated the contents of the white paper.[118]

### 4.4 *South Africa*

Whilst various structures had been created to deal with cyber security issues, South Africa lacked a holistic cyber mode of operations until recent-

[112] CERT stand for Computer Emergency Response Team.

[113] Australian Government 2009, p. i-vii.

[114] Australian Government 2009, p. vii.

[115] Waters, Ball and Dudgeon 2008.

[116] Australian Department of Defence 2009b, p. 83.

[117] Hanna 2009, p. 106.

[118] Australian Department of Defence 2009a.

ly.[119] Security specialist Alpha Wolf explains on the blog of the Information Security Group of Africa that the South-African Cabinet approved a National Cyber Security Policy Framework in March 2012. The framework makes provision for the establishment of a number of structures and institutions to coordinate the activities of various security cluster departments already working on a wide range of issues. The framework tasks the state security agency with overall responsibility for developing, implementing and coordinating South Africa's cyber security measures as an integral part of its mandate, and it aims at:

- addressing national security threats in cyberspace;
- combating cyber warfare, cyber crime and other cyber ills;
- developing, reviewing and updating existing substantive and procedural laws to ensure alignment;
- building confidence and trust in the secure use of information and communication technologies.[120]

## 5. Conclusion

This Chapter's purpose was to portray the various views used by a number of states and one major institution (NATO) to counter threats coming from, or directed against the cyber domain. To that end allies and other stakeholders have been examined; from a general cyber security perspective, as well as from a military angle.

Although major differences are obvious at first sight, a number of observations can be made. First, a number of states is in the process of developing an overarching cyber security strategy, as well as a 'military' cyber strategy. Secondly, it is interesting to note that whether formally referring to cyber or 'informatization', cyber is seen and treated substantively as more than 'computer communication', at least in military doctrines. Thirdly, different terms are used amongst the nations, even amongst the members of NATO. Furthermore, whereas some states explicitly mention cyber security as a prerequisite for economic prosperity, others emphasise cyber security as a condition for (domestic) stability.

Generally, most states seem to apply a holistic approach in cyber security, acknowledging that cyber threats may have different sources, intentions, targets, and vectors or avenues of 'attack', and require public efforts

[119] Tikk 2011, p. 237.
[120] Wolf 2012.

as well as private exertion in response to threats. Their approach is also holistic since it combines various agencies in anticipation to cyber threats.

The comprehensiveness of cyber security policies also underlines the fact that security is no longer to be viewed as dichotomous, separating internal and external security, but that security rather is the integration of security for, and in all vital interests of states involved.

Moreover, cyber also provides states and NATO with opportunities, as it offers new techniques, sources of information, means of communication, economic growth, trade opportunities, as well as weapons and angles (and targets) of 'attack'. To that end, most States, either implied or explicitly affirmed, pay attention to defensive as well as offensive policies (including policies to enhance intelligence opportunities).

Finally, even in times of economic recession or budget cuts within government, it is also clear that states are willing to invest in the cyber domain and cyber security, which stresses the importance of the cyber threat.

## 6. References

Australian Department of Defence (2009a), 'Australian Chief of Defence Force and Secretary of Defence, Round Table Discussion for the Federal Government's Defence White Paper', 7 May 2009, MSPA 90507/09, at: <www.defence.gov.au/media/SpeechTpl.cfm?CurrentId=9069>.

Australian Department of Defence (2009b), 'Defending Australia in the Asia Pacific Century: Force 2030, Defence White Paper 2009', Canberra (AUS): Defence Publishing Service, at: <www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf>.

Australian Government (2009), 'Cyber Security Strategy', Attorney General's Department, at: <www.ag.gov.au/cca>.

Baocun, Wang and Li Fei (1995), 'Information Warfare', in: *People's Liberation Army Daily*, June 20, <www.fas.org/irp/world/china/docs/iw_wang.htm>.

Billo, C.G. and W. Chang (2004), *Cyber Warfare – An Analysis of the Means and Motivations of Selected Nation States*, NH: Institute for Security Technology Studies at Dartmouth College.

Bundesministerium des Innern [Federal Ministry of the Interior] (2011), *Cyber-Sicherheitsstrategie für Deutschland* [Cyber Security Strategy for Germany], February, Berlin (DEU): Bundesministerium des Innern/Media Consulta Deutschland GmbH, <www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile>.

Carr, J. (2012), *Inside Cyber Warfare: Mapping the Cyber Underworld*, Beijing: O'Reilly.

Coker, C. (2009),*War in an Age of Risk*, Cambridge: Polity Press.

comScore.com (2009), 'Russia Has World's Most Engaged Social Networking Audience', 2 July, <www.comscore.com/Press_Events/Press_Releases/2009/7/Russia_has_World_s_Most_Engaged_Social_Networking_Audience> (Accessed 11 May 2012).

Daily Mail (2011), 'Armed Forces chief to set up UK cyber warfare unit to launch attacks on enemies in cyberspace', in: *Mail Online (Daily Mail),* 9 January, <www.dailymail.co.uk/news /article-1345490/Armed-Forces-chief-set-UK-cyber-warfare-unit-launch-attacks-enemies-cyberspace.html>.

Delon, F. (2011), *Stratégie de la France: Défence et sécurité des systèmes d'information* [French Strategy for the Defence and Security of Information Systems], Paris (FRA): Agence Nationale de la Sécurité des Systèmes d'Information, <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf>.

Dylevsky, I.N. et al. (2007), in: *Moscow Military Thought*, March 31.

Ghioni, F. (2012), 'New Joint Cyber Concept, Blessed by STRATCOM, Nears Dempsey's Desk', in: *Fabio Ghioni's Official Website*, 10 April, <www.fabioghioni.net/blog/2012/04/10/new-joint-cyber-concept-blessed-by-stratcom-nears-dempseys-desk/>.

Giles, K. (2011), 'Information Troops' – a Russian Cyber Command?', in: C. Czosseck, E. Tyugu and T. Wingfield (eds.), 2011 3rd International Conference on Cyber Conflict, Tallinn: CCD COE Publications, p. 45-60.

Goble, P. (1999), 'Russia: Analysis from Washington – A Real Battle on the Virtual Front', *Radio Free Europe/Radio Liberty* (11 October), <www.rferl.org/content/article/1092360.html>.

Goetz, J., M. Rosenbach and A. Szandar (2009), 'National Defense in Cyberspace', in: *Der Spiegel Online International*, 11 February, <www.spiegel.de/international/germany/0,1518,606987,00.html>.

Gorman, S. (2010), 'U.S. Backs Talks on Cyber Warfare', in: *Wall Street Journal* 4 June, <online.wsj.com/article/SB10001424052748703340904575284964215965730.html>.

Gorman, S. and J. Barnes (2011), 'Cyber Combat: Act of War, Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force', in: *Online Wall Street Journal*, 30 May, <online.wsj.com/article/SB10001424052702304563104576355623135782718.html>.

Hagestad, W.T. II (2012), 'The Chinese Government & People's Liberation Army's Use of Information Warfare (IW) – Cyber Warfare', ITGP, <www.infosecisland.com/download/index/id/63.html>.

Hanna, C. (2009), 'Cyber Operations and the 2009 Defence White Paper: Positioning the Australian Defence Organisation to Be Effective, Transparent and Lawful', in: 5 *Security Challenges*, No. 4, p. 103-117, <www.securitychallenges.org.au/ArticlePDFs/vol5no4Hanna.pdf>.

Hoover, J.N. (2011), 'White House Comprehensive Cyberspace Policy', in: *InformationWeek Government*, 16 May, <www.informationweek.com/news/government/policy/229500>.

Hughes, R.B. (2009), 'NATO and Cyber Defence', in: *Atlantic Perspective*, No. 1.

Kissinger, H. (2011), *On China*, New York: The Penguin Press.

Krekel, B. (2009), *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corporation, prepared for the US-China Economic and Security Review Commission of the United States Congress, <www.uscc.gov/researchpapers/2009/Northrop-Grumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

Krekel, B., P. Adams and G. Bakos (2012), 'Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage', Northrop Grumman Corporation, prepared for the US-China Economic and Security Review Commission of the United States Congress (March 7, 2012), <www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf>.

Lewis, J.A. and K. Timlin (2011), *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*, Washington, DC: Center for Strategic and International Studies.

Ministère de la Défense [French Ministry of Defence] (2008), 'Défense et Sécurité nationale, Le Livre Blanc' [The French White Paper on defence and national security], Paris (FRA): Odile Jacob Publication, <www.defense.gouv.fr/portail-defense/enjeux2/politique-de-defense/livre-blanc>.

Mshvidobadze, K. (2011), 'The Battlefield on Your Laptop', *Radio Free Europe/Radio Liberty*, 21 March, <www.rferl.org/articleprintview/2345202.html>.

NATO (2008), 'Bucharest Summit Declaration', issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April, <www.nato.int/cps/en/natolive/official_texts_8443.htm?selectedLocale=en>.

NATO (2009), 'Riga Summit Declaration', issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006, <www.nato.int/cps/en/natolive/official_texts_37920.htm?selectedLocale=en>.

NATO (2010), 'Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization', adopted by Heads of State and Government at the NATO Summit in Lisbon, 19-20 November, Brussels: NATO Public Diplomacy Division, <www.nato.int/cps/en/natolive/official_texts_68580.htm>.

NATO (2012), 'Press Conference by NATO Secretary General Anders Fogh Rasmussen and Supreme Allied Commander Transformation General Stéphane Abrial at the SACT Seminar', February, <www.nato.int/cps/en/natolive/opinions_84671.htm?selectedLocale=en>.

NATO Allied Command Transformation (2012), *Cyber Defence Burden-Sharing Concept (Draft)*, Norfolk, VA.

NATO Defence College (2010), 'Understanding the Georgia Conflict, Two Years on Reviews and Commentaries', Rome: NATO Defence College, September, <www.ndc.nato.int/research/series.php?icode=9>.

Oakley, J.T. (2011), 'Cyber Warfare: China's Strategy to Dominate Cyberspace', Fort Leavenworth, KS: U.S. Army Command and General Staff College, <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA547718>.

Noshiravani, R. (rapporteur), (2011), 'NATO and Cyber Security: Building on the Strategic Concept, Workshop Report', Chatham House, <www.chathamhouse.org/sites/default/files/public/Research/International%20Security/200511nato.pdf>.

President of the United States (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

PRC Embassy in Washington DC (2006), 'China Maps Out Informatization Development Strategy', 11 May, <www.china-embassy.org/eng/xw/t251756.htm>.

Qiao Liang and Wang Xia (2002), *Unrestricted Warfare: China's Master Plan to Destroy America*, Pan American Publishing Company.

SCO (2011), 'Joint Communiqué of Meeting of the Council of the Heads of the Member States of the Shanghai Cooperation Organisation Commemorating the 10th Anniversary of the SCO', (Astana, 14-15 June), <www.sectsco.org/EN/show.asp?id=293> (Accessed 18 May 2012).

Schmidt, H.A. (2011), 'Launching the U.S. International Strategy for Cyberspace', in: *The White House Blog*, 16 May, <www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>.

Stokes, M.A., J. Lin and L.C.R. Hsiao (2011),*The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute (November 11).

Talbot, D. (2010), 'Russia's Cyber Security Plans', 16 April, <www.technologyreview.com/blog/editors/25050/>.

Thomas, T.L. (2005), *Cyber Silhouettes: Shadows over Information Operations*, Fort Leavenworth: Foreign Military Studies Office.

Tikk, E. (2011), *Frameworks for International Cyber Security, National Cyber Security Policies and Strategies*, Tallinn: CCD COE Publications.

Tikk, E., K. Kaska and L. Vihul (2010), *International Cyber Incidents: Legal Considerations*. Tallinn: CCDCOE.

UK Government (2010), *Securing Britain in an Age of Uncertainty*, presented to Parliament by the Prime Minister by Command of Her Majesty, October, Norwich, UK: The Stationery Office.

UK Government (2011), *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: UK Government's Cabinet Office, <update.cabinetoffice.gov.uk/resource-library/cyber-security-strategy>.

UK Prime Minister's Office (2010), 'Strategic Defence and Security Review: Prime Minister David Cameron has unveiled details of the Strategic Defence and Security Review (SDSR)', in: 10 *The Official Site of the British Prime Minister's Office*, 19 October, <www.number10.gov.uk/news/strategic-defence-review/>.

United States Strategic Command (2012), 'Cyber Command Fact Sheet', at: <www.stratcom.mil/factsheets/cyber_command/>.

US Department of Defense (2003), 'Annual Report on the Military Power of the People's Republic of China 2003', 28 July, <www.defense.gov/pubs/2003chinaex.pdf>.

US Department of Defense (2011a), 'Annual Report to Congress on the Military and Security Developments Involving the People's Republic of China 2011', <www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf> (Accessed: 13 May 2012).

US Department of Defense (2011b), 'Joint Concept on Cyberspace', draft version, Washington, DC: Joint Staff Publication.

US Embassy London (2012), 'Joint Fact Sheet: US-UK Progress towards a Freer and More Secure Cyberspace' (White House Office of the Press Secretary), *U.S. Embassy in London Official Website*, <london.usembassy.gov/gb169.html>.

Waters, G., D. Ball and I. Dudgeon (2008), 'Australia and Cyber-Warfare', Canberra: ANU E Press (The Australian National University), <epress.anu.edu.au/sdsc/cyber_warfare/pdf/whole_book.pdf>.

Wolf, A. (2012), 'Cabinet Approves National Cyber Security Policy Framework', in: *Blog of the Information Security Group of Africa*, 13 March, <www.isgafrica.org/blog/archives/1282>.

Xinhua.net (2004), 'Jiang Zemin Stresses Information Technology in Army Construction', July 26, <http://news.xinhuanet.com/english/2004-07/26/content_1651552.htm>.703>.

# Contributors

**Dr. Floribert H. Baudet** is Associate Professor of Strategy (Section Military History and Strategy) at the Netherlands Defence Academy (Faculty of Military Sciences).

**Dr. Robert J.M. Beeres** is Associate Professor of Defence Accounting Control & Economics at the Netherlands Defence Academy (Faculty of Military Sciences) and at Nyenrode Business Universiteit.

**Dr. Myriame T.I.B. Bollen** is Associate Professor in organisation studies at the Netherlands Defence Academy and a member of the Board of the Faculty of Military Sciences. Since 2004, she is a visiting professor at the Baltic Defence College, Estonia.

**Lieutenant-Colonel A.J.H. (Han) Bouwmeester MSc MMAS** is an operational concept developer and a core member of the Cyber Defence project team at NATO's Allied Command Transformation in Norfolk (VA, USA).

**Dr. Theo B.F.M. Brinkel** is acting Head of the International Securities Studies at the Netherlands Defence Academy (Faculty of Military Sciences).

**Dr. Elly Broos** is Assistant Professor of Human Resource Management at the Netherlands Defence Academy (Faculty of Military Sciences).

**Colonel dr. Paul A.L. Ducheine LL.M.** is Associate Professor of Cyber Operations at the Netherlands Defence Academy (Faculty of Military Sciences), (guest) lecturer in Military Law at the University of Amsterdam, and researcher at the Amsterdam Centre of International Law. More at: <home.medewerker.uva.nl/p.a.l.ducheine/>.

*P. Ducheine, F. Osinga and J. Soeters (eds.), Cyber Warfare: Critical Perspectives*

**Dr. Paul C. van Fenema** is Associate Professor of Management & Organisation at Netherlands Defence Academy (Faculty of Military Sciences). More at: <www.paulcvanfenema.com>.

**Colonel ir. J.M. (Hans) Folmer MSS** is the Commanding Officer of Task Force Cyber at the Netherlands Ministry of Defence.

**Professor dr. Terry D. Gill** is Professor of Military Law at the University of Amsterdam and the Netherlands Defence Academy (Faculty of Military Sciences).

**Henk de Jong MA** is an Assistant Professor of Military History at the Netherlands Defence Academy (Faculty of Military Sciences).

**Professor dr. ir. Robert E. Kooij** is principal scientist at TNO (Netherlands Organisation for Applied Scientific Research) and part-time professor Robustness of Complex Networks at the Delft University of Technology.

**Dr. Sean Lawson** is an Assistant Professor, Department of Communication, University of Utah. More: <www.seanlawson.net>.

**Dr. ir. Roy H.A. Lindelauf** is an Assistant Professor of Military Operational Art & Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).

**Professor dr. Jan S. van der Meulen** is an Associate Professor at the Netherlands Defence Academy (Faculty of Military Sciences), as well as a professor of military-societal studies at Leiden University (Faculty of Social and Behavioural Sciences).

**Dr. René Moelker** is Associate Professor of Sociology at the Netherlands Defence Academy (Faculty of Military Sciences).

**Dr. Herman Monsuur** is Associate Professor of Mathematics and Operations Research at the Netherlands Defence Academy (Faculty of Military Sciences).

**Air-Commodore prof. dr. Frans P.B. Osinga** is Professor of Military Operational Art & Sciences, and Chair of the War Studies Department at the Netherlands Defence Academy (Faculty of Military Sciences).

**Dr. Thomas Rid** is a Reader in War Studies at King's College London and a non-resident fellow at the Center for Transatlantic Relations at the School for Advanced International Studies (SAIS), Johns Hopkins University, Washington, DC. More at: <thomasrid.org>.

**Dr. Maarten G.D. Rothman** is Associate Professor of International Security Studies at the Netherlands Defence Academy (Faculty of Military Sciences).

**Professor dr. Joseph M.M.L. Soeters** is Professor of Management and Organisation Studies at the Netherlands Defence Academy and Tilburg University, and Chair of the Department of Management, Organisation and Defence Economics (Faculty of Military Sciences).

**Lieutenant-colonel Jan F. Stinissen LL.M.** is a Senior Analyst to NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia.

**Lieutenant-colonel Nico W.A. Timmermans** is Assistant Professor of Military Operational Art & Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).

**Dr. Giliam G. de Valk** is Associate Professor Intelligence & Security Studies at the Netherlands Defence Academy (Faculty of Military Sciences), and lecturer at the University of Amsterdam (Faculty of Science – Institute for Interdisciplinary Studies).

**Professor dr. ir. Piet F.A. Van Mieghem** is Professor of Telecommunication Networks and chairman of the section Network Architectures and Services (NAS) at the Delft University of Technology.

**Lieutenant-colonel Joop E.D. Voetelink LL.M.** is an assistant professor of Military Law at the Netherlands Defence Academy (Faculty of Military Sciences).

**Prof. dr. Ad L.W. Vogelaar** is Professor of Military Behavioural Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).