CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org.uk
F: +44 (0)20 7957 5710 www.chathamhouse.org.uk
Charity Registration Number: 208223

NATO OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

Rapporteur Report

NATO and Cyber Security: Building on the Strategic Concept

20 May 2011

Rapporteur: Reyhaneh Noshiravani

Introduction

This workshop on 'NATO and Cyber Security: Building on the Strategic Concept' brought together a group of senior officials from NATO, national governments, industry, and academia. The goal of the event was to discuss and examine the strategic dimensions of potential cyber threats to the land, sea, air, and space domains of NATO's collective security umbrella. Participants discussed possibilities for mitigating various types of cyber threats, while looking at options for deterrence and collective defence and security in the cyber domain. They examined opportunities for the implementation of new strategic approaches to cyber threats, and the ways these approaches could feed into the new Strategic Concept.

Overview of the Cyber Problem

The meeting opened with a general discussion of cyber security risks and threats, and NATO's potential role and ability to tackle these problems both inside and outside the Alliance system. The cyber domain was described as an environment that is easily penetrable and accessible, and one that allows for the rapid proliferation of information and diffusion of opponents. This has profound implications for national and international security and is transforming traditional notions of conflict and warfare. The theatre of operations in cyber space is a global one where actors are contiguous even though their geographical proximity may vary widely. There is a broad range of possible malicious or hostile actions in cyberspace, including crime, espionage, overt cyber attack and hacktivism. The primary vulnerabilities were described as being related to intelligence and information security, as uncertainties in attribution and potential responses by opponents render attacks indecisive. Nevertheless, the possibility of eroding an opponent's resistance gives cyber attacks the potential to become serious military threats. Accordingly, it was agreed there is a growing need to formulate security policy that deters malicious cyber activities by demarcating thresholds and establishing a framework for regulating cyberspace.

Participants also agreed that governments should address these issues through cross-sector cooperation and actively seek collective intelligence beyond the parameters of a traditional security approach. As an international security organization, NATO is not only obligated to examine this problem but may also be uniquely positioned at the forefront of shaping the cyber environment.

Four principal challenges were identified that NATO faces when formulating an effective cyber security policy:

- Overcoming imprecision in terminology by formulating standard definitions of what constitutes an attack, war or use of force in cyberspace.
- Bolstering governance by creating a strategic framework for managing crises in a timely manner. This includes delineating responsibilities at both the national and international levels, potentially adapting laws of war for a new mode of conflict, and addressing trade issues.
- Formulating norms of behaviour to facilitate regulation of cyberspace. This requires a multilateral approach that includes increased

harmonisation of national strategies, and facilitating information sharing on threat mitigation.

- Balancing between collective security and protection of individual liberties. It was noted by participants that the two principles are not mutually exclusive and can in fact complement each other.

The meeting continued with an examination of NATO's current cyber security policy, the importance of and potential for cross-sector cooperation, and the role of international law in mitigating potential problems.

The New NATO Cyber Security Policy

Although NATO has long been protecting its communication and information architecture, the 2002 Prague Summit placed cyber defence on the Alliance's political agenda for the first time. A series of cyber attacks on Estonian public and private institutions in 2007, and the 2008 conflict between Russia and Georgia gave this matter further urgency, as they revealed the potential of cyber attacks as a major component of conventional warfare. The development and use of destructive cyber tools that can threaten national and transatlantic security and stability emphasised the need for stronger defence of the information and communications technology (ICT) infrastructure of NATO and its member states. This in turn prompted NATO to broaden the scope of its strategy and formulate a new cyber defence policy (which was in the final stages of drafting when this workshop took place, and was approved on 8 June 2011).

The revised policy offers a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber attacks and bolstering the resilience of existing networks. In its efforts to achieve this, the new policy is twofold: allies are responsible for the safety and security of their own ICT systems, as the strength of a collective cyber defence strategy is dependent on the security of its weakest link. In addition, the policy encourages a framework for cooperation and assistance among the allies for the protection of their ICT networks and systems. This includes collaboration on a number of fronts including optimized information sharing, situational awareness, and secure interoperability based on agreed sets of standards. Moreover, it improves the coordinated protection of NATO structures and devises new political and operational mechanisms for responding to cyber attacks. Finally, it outlines principles of NATO cooperation with partner countries, international organizations, the private sector and academia to bolster cyber security.

One participant commended the new policy for its increasingly comprehensive approach to cyber security. The directive to regard all missions in light of cyber defence presents a welcome development in NATO's approach to security. It was noted that, by identifying protection as its principal mandate and formulating mechanisms for training and education, the policy provides the best means of deterrence currently available. And by contributing to the norms of acceptable cyber behaviour it bolsters cooperation and collaboration between NATO and its member states.

While these are significant strides in NATO's approach to cyber security, participants identified several factors that continue to adversely influence the policy's resilience. First, the inherent interdependencies within cyber space blur the boundaries of responsibilities. This has the potential to undermine trust within the alliance by leading to blame shifting in the event of a cyber-related crisis. Secondly, advance warning is not contained within a central approach and still takes place on a bilateral basis between NATO and member states, which hinders communication and slows response processes. Finally, at present there are insufficient resources for implementing the policy, which directly impacts its efficacy.

Government and Industry Relations

Discussants observed that only recently have governments and the private sector begun to appreciate the inherent risks generated by heavy dependence on cyberspace. Ambiguities on the division of responsibility between sectors and differing objectives have led to uneven cooperation and response. It was noted that, on the one hand, governments may represent the main actors capable of addressing the growing need for a standard model of cyber risk management. On the other, the private sector's primary objective is to deliver value to its shareholders and it is naturally reluctant to accept additional regulatory measures. For multinational companies this situation is compounded by the complex and varying legal and regulatory frameworks they must cope with.

Nevertheless, participants agreed that the private sector should accept a certain degree of responsibility for protecting the integrity of networks upon which the public sector – including the military and financial institutions – relies. Therefore, the private sector should work to reduce vulnerabilities, improve quality, and enhance cyber security best practice in the management and provision of goods and services.

Another impediment for engaging the cooperation of the private sector was the lack of common understanding of the cyber problem. Since the private sector is incentivised to operate differently from governments in cyberspace, cyber risks must be presented to them as having the potential to effect processes that are core to business, such as revenue streams, brand and reputation, and continuity of supply chains. Formulating a common lexicon is an important step in promoting cross-sector cooperation. Elevating the conversation about cyber security to the boardroom level is a critical step, as it will encourage the issue to be considered across an organisation, instead of being the sole responsibility of the ICT department.

While numerous obstacles persist, participants agreed that there are ample opportunities for cross-sector cooperation. Moreover, since many private sector organisations are global actors, NATO could play an important role in fostering this partnership.

Regulation, Law, and International Co-operation

Participants observed that any NATO cyber defence policy must confront issues pertaining to international laws and laws of armed conflict. Consequently, the policy needs to establish a clear objective and some level of consensus on the standards that member states will apply. This includes developing thresholds that address the following questions:

- What amounts to the 'use of force' in the cyber domain?
- When does a cyber attack amount to an armed attack?
- What is the permitted response to a computer network attack?
- What body of law applies to those responses?

There is a need for coordination among member states on defining use of force under Article 4 of NATO's charter. While the UN charter does not directly apply to NATO, it does affect member states. Therefore it is important to identify when computer network attacks amount to armed attacks under Article 51 of the UN charter, and by extension Article 5 of the Washington Treaty.

According to one participant, within the framework of international law, the use of force generally means armed force. Economic and political coercion and espionage fall outside existing legal parameters. There was general consensus among participants that a cyber attack would be considered use of

armed force if it produced a physical consequence such as human injury or destruction of critical infrastructure. One discussant noted that, according to international law, the use of force does not have to be direct. It can be by proxy or the supply of weapons and logistical support for activities that constitute the use of force. Therefore, as long as a state's requisite level of involvement or control of actors can be proven then it can legally be held accountable for the use of force.

Participants agreed that attribution is another threshold with legal ramifications. The existing problems in identifying attackers within cyberspace continue to affect the ability of states and organizations such as NATO to respond in a timely and legal manner. This problem will be further complicated with expanding cyber infrastructure and growing number of users.

Attribution is also important because it determines the permitted response to a cyber attack. It was noted that, in the event of the use of armed force by a non-state actor, NATO consultation under Article 4 could lead to the conclusion that military action short of collective self-defence was required. Any cyber policy must also identify when an attack falls within the parameters of laws of armed conflict, and standards should attempt to identify the involved actors. The question of shrinking defence budgets and outsourcing of security measures was raised, and it was noted that NATO should be cautious of the dependency created by this outsourcing.

Participants noted that the efficacy of any NATO security policy could be buttressed through cooperation with the European Union (EU). Membership overlap between these organizations has a practical effect on their scope of competence, as there are a range of issues on which the EU concurs with NATO, or has exclusive competence which effects the latter's capabilities. Many EU provisions which are termed exceptions for the defence sector shrink the competence of nations as the European Court of Justice often has a narrow reading of exceptions to give broadest scope to community law.

This has a significant impact on the ability of NATO's EU members to contribute to decision-making within the alliance. Moreover, the EU can implement supranational legislation, which is directly binding for member states and can conclude intergovernmental arrangements, as it is a member of the WTO. Concurrently, NATO can theoretically conclude international agreements, which from an international legal perspective presents an innovative way of supplementing existing international law with practice. This

could influence the meaning of international principles and rules pertaining to the use of force and armed attacks.

However, there are also impediments to EU-NATO cyber security cooperation. NATO's principal mission is to safeguard the freedom and security of its members through political and military means. Though the EU has a common security and defence policy (CSDP) it is primarily an economic organization. Moreover, its defence policy tends to remain within a law enforcement model which emphasises individual freedoms and rights. Malicious and hostile activity in cyberspace covers a wide spectrum and do not differentiate between law enforcement and defence. Thus, the differing mandates of the respective agencies separate their spheres of competence and places legal limits on their ability to cooperate in this area.

While NATO-EU cooperation has the potential to bolster cyber governance, it alone is not sufficient. The interconnected and interdependent nature of cyberspace subverts legal discussions among organizations that represent the interests of a select group of states. Since EU or NATO legislation can have transnational ramifications, any discussion of the subject needs to transcend these organizations. While this complicates regulatory measures, participants stressed that there is a level of consensus among states on issues of cyber governance, which can be exploited. Such efforts can take place on a multilateral basis and include governments, the private sector and civil society.

Participants concluded that NATO is in a position to carve out a unique niche in global cyber security. Nevertheless individual states remain the principal actors in cyber security and at the forefront of confronting related issues. International organizations can serve as forums to facilitate government coordination and establish common lexicons and norms. While international treaties can act as strategic instruments, they will be ineffective if nations do not clearly define treaty missions and objectives. There is no shortage of existing legislation, but what is currently lacking is the ability to implement the existing laws across the spectrum. No one has a silver bullet, but everyone can make a positive contribution. Finding aligned incentives and areas for cooperation across the public and private sectors and civil society is the key to progress on cyber security.