EWG 17 - Eurodefense Working Paper – Cyber security – no front line

Executive Summary

More than any other area of defence policy, the cyber domain requires extensive co – operation with civilian agencies and commercial contractors. Defence structures should adopt an open door approach to exploring developments in this field. National Security considerations will still apply, and sensitive information will need safeguarding.

Recommendations

- As well as defence assets, Critical National Infrastructure will need protecting. In the cyber domain there is no front line.
- Defending a country's economic wellbeing may be considered to be a matter for its National Security apparatus.
- Allies should co-operate in developing a software protocol that can trace the route of a cyber-attack, or a cybercriminal, to show that there is no hiding place in the cyber domain.

Introduction

Many will be familiar with developments in the field of electronic warfare. Recently the simple act of detecting and jamming an enemy's signal was a war winner. During the Cold War developments in satellite technology led to another dimension in intelligence gathering and signals transmission. Recently this trend has been augmented, with the advent of powerful computers and processing systems. Any country wishing to protect itself now needs to have a well developed electronic and IT capability at its disposal. Cyber warfare made its presence known via the cyber attacks on Estonia (2007) and Georgia (2008). More recently the Stuxnet attack on Iranian nuclear facilities has been attributed to this new form of warfare.

Threats

In addition to "classic" defence threats related to loss of sensitive information and the disruption of command and control systems, the cyber domain poses risks to the way a modern society operates. Infrastructure such as smart energy grids, control systems for power stations and water works are all vulnerable to differing kinds of cyber attack. All of these points could be attacked by an enemy seeking to coerce without resort to war. Modern society is increasingly dependent on IT systems for its everyday use; from service delivery by local authorities to on-line shopping by consumers, daily life would quickly become totally chaotic should a large scale attack on a country disable its cyber based nervous system.

Policy Developments

The response was initially unco-ordinated. Operational units such as the US's Cyber Command were established ahead of a fully articulated strategy. Cyber strategies were formulated in a variety of countries: the UK initially in 2009 and again in 2011, the US, France and Luxembourg in 2011 and Germany in 2012. Agencies, such as the EU and NATO have sought to acquire a competence in this field.

NATO: As early as 2002 NATO began to address the cyber threat at the Prague summit. Following the Estonia and Georgia attacks, the Alliance established an Estonian based centre for excellence in 2008; a non-operational element. The New Strategic Concept promulgated at the Lisbon summit of November 2010 calls for the Alliance to be fully capable in the face of this new threat. On 1st July 2012 the NATO Communications and Information Agency (NCIA) was established. This will endeavour to keep the Alliance's Information systems secure.

It will be clear from this recitation of dates and developments that policy in this area is evolving swiftly. In effect Moore's law which only applied to IT and computing has transferred to the policy arena. Therefore the Alliance needs to adopt a framework approach which will ensure that all the relevant commands and agencies are fully informed of developments. This should work on a "patch" basis to ensure immediate protection, but underlying this should be a policy approach which requires countries to fully share information about threats and remedies.

EU: The EU effort in this area is reflected by its shared competencies: The European Council, EP and EC. Due to the dual nature of this domain (defence and law enforcement) there is a greater risk of duplication of effort. The Justice and Home Affairs (JHA) dossier will consider the legal and criminal aspects of cybercrime, while the Common Security and Defence Policy dossier will be concerned with the relevant defence implications. The European Defence Agency should be the recognized centre of excellence for the EU, similar to its NATO counterpart. The EDA has Cyber security as one of its top 10 priorities. Budgetary matters for the further finance of this function should be resolved as a matter of priority.

Principal challenges

Doctrine: an agreed doctrine should be established between EU agencies and NATO. The first priority should be the internal safeguarding of information within EU and NATO systems (Information Assurance or IA). Secondly NATO and the EU should development a resilience based approach; assuming that their systems have been compromised, and protecting vital information. The promulgation of an agreed doctrine will signal the importance of this threat to all involved at every level throughout both agencies. This will, in turn, apply to those agencies which deal directly with NATO and the EU; in effect this will spread best practice throughout the supply chain / ecosystem of related agencies and contacts.

Legality: The Council of Europe agreed on the Budapest Convention on cyber crime in 2001. National governments and agencies are now engaged in establishing legally binding norms or codes of conduct with regard to the safeguarding of intellectual property, and the illegal transfer of data between jurisdictions. This is intended to prevent criminals or non-state actors profiting from stolen information. It also acts as a legal means to prosecute people for industrial espionage on behalf of third parties. However, the technology to identify the ultimate perpetrator of such acts is, as yet, elusive.

Co-operation architecture

International efforts are underway to establish "rules of the road" to avoid a cyber arms race or a cyber war by miscalculation. Both the EU and NATO should lend their good offices to ensure that such efforts are productive. EU and NATO applicants should agree to accede to existing protocols with regard to cyber security and cyber crime.

The future

European countries are now well aware of the extent of the cyber threat. All government agencies and infrastructure providers should be in compliance with basic cyber security measures. The ability of NATO and EU agencies to safeguard their IT and communication systems will depend on their combined Research and Development efforts. This must be addressed through appropriate levels of funding, either through state channels or via co-operative ventures with industry and academia.

Way forward

- At the European level Allies and partners must co-operate across policy areas and organizational boundaries to safeguard information and systems.
- Agreed common standards will be the best defence. A well-managed operation will help to prevent cyber intrusion. This will enable western allies to retain their critical advantage.
- A comparison of national cyber doctrines and the NATO and EU guidance will enable weaknesses to be spotted in individual organizations or national agencies.
- In a time of budgetary constraint, co-operation between agencies should be encouraged to ensure the maximum value from public expenditure, and to avoid differing regimes emerging. Cyber criminals and non-state actors will be looking for weak spots.