# Cyberspace: Criminals or Enemies?

NATO paper outline, Professor Michael Levi

Bruce Schneier noted that “Security is both a feeling and a reality. The propensity for security theater comes from the interplay between the public and its leaders. When people are scared, they need something done that will make them feel safe, even if it doesn't truly make them safer. Politicians naturally want to do something in response to crisis, even if that something doesn't make any sense.” Not British politicians, obviously!!!

Current insecurity concerns are real enough, on Europe’s border – Ukraine – and on NATO’s border – Ukraine and Islamic State. But the urge to be seen to be doing something is powerful, and should be accompanied by actually doing things that are effective, even if few people know about them. Deterrence – whether of crime or invasion – involves ‘credible threat’, i.e. alarming ‘the enemy’ that you can do something to them that will stop them doing what they want and that they will be really sorry for trying.

Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks. The NATO National Cyber Security Framework Manual (2012) makes it clear that there are different constructions of national security and even of cyberspace within the NATO family. Communications and Information Security (CIS) is defined as the ability to *adequately* [my italics] protect the confidentiality, integrity and availability of CIS and the information processed, stored or transmitted. NATO defines ‘cyber defence’ as ‘the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace.’ This talk will not exhaustively review that Manual or its core discussions: suffice it to state that we need to work out how much protection is ‘enough’, and what level of intrusion and damage is sufficient to merit different levels of response from Member States individually and from NATO collectively. The recent House of Commons Defence Committee criticisms about rethinking NATO are apposite here.

So are cybercriminals enemies or just criminals? They can be both or either, or can see themselves as neither enemies nor criminals, but just playing and exploring. (Disputes over intentions are part of the media debate in extradition cases, but harms are not always correlated with intentions – you can wipe someone out carelessly, and you can totally fail to meet your intentions. And as in Ukraine, countries usually want to deny culpability for cyber-attacks and have some skills to do so.)

For a long time, NATO has had to deal with the shift to asymmetric warfare, towards (in the words of a classic 2001 Rand study) Networks and Netwars. Many international relations scholars remain wedded to the distinction between national security and human security, but in a globalised world economy, it is hard enough to decide which companies to protect in the national interest – when a Japanese company invests in Wales, it is proper for us to seek to protect its interests as much as a British company that invests abroad - and the slippery slope between protecting corporate interests and protecting national interests becomes quite a complex task. Unless we can define national security independently, this often turns out to be mainly about our focus of interest, since economy, society and sovereignty are so intermingled and internationalised in the contemporary era.

The protection of critical national infrastructure depends on judgments about (1) what is ‘critical’ and (2) what level of protection we want (or what level of electronic invasion we are prepared to tolerate). This still smacks somewhat of the Maginot line concept of absolute, binary protection, whereas for many purposes, we would do better to think of risks as linear, except for the leaking of some secrets. Industrial secrets might be thought of as binary risks, but even if ‘stolen’[[1]](#footnote-1) electronically or by corruption/blackmail, some of them may not be as easy to recreate and use or sell in the open marketplace as one might think. An example is the conflict between Apple and Samsung over alleged copyright violations. The more that China and Russia develop, the more they will look to enforcement of their own IP rights – but inconsistency is possible!

The situational culpability is made more difficult when key economic actors are in the hands of the State, and so commercial espionage and DDOS attacks can easily shift between inter-corporate conflicts and inter-statal ones. Explanations of motivation are often tinged with what we want them to be, but it is important to avoid monocausal accounts: there is no reason why motives cannot be both political and personal (like greed), though ‘home cultures’ may seek to discipline either of these if they suspect they are interfering with the work. The fuzziness of the line between state, state-sponsored and state-tolerated cybercrimes can be explored within the range of NATO doctrines.

The *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation* of November 2010 recognises that malicious cyber activities ‘can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability’. Looking at the current situation in the Middle East and Ukraine, let us think about how cyber issues relate. Obviously there are all kinds of SIGINT that might be described as cyber from all sides which may or may not be revealed to show who shot down whom; communications from all sides are usually involving some cyber-dimensions, even if it is only travel; and cyber-messages in SWIFT and other financial transfers may be deceitfully changed to conceal transmission data, as various investigations have shown into the misconduct of major international banks in sanctions violations. Meanwhile, in the background, cyber attacks for financial gain go on which may weaken our capacity or willingness to afford wars. So we need to distinguish between cyber attacks that reduce the capacity and willingness to engage in offence or defence; and cyber attacks that reduce operational strength of either side (or sides) in a conflict.

Much crime has gone on to finance IS (and in a different way, Russia – though corrupt money flows *out of* China and Russia are hardly ways of strengthening those regimes). But frankly, when so much *materiel* can be seized from fleeing soldiers, cybercrime to generate fighting funds is relatively unnecessary. What NATO and MS might aim for would be technological disablers of one’s own kit for precisely that situation – provided no internal traitors or external hackers find out how it works. There is nothing new about Arms Races in technology – but what is newer is that treason apart, it is getting harder to tell or to publicly *prove* without revealing intelligence sources whether your enemy or a third party is committing the intrusion. In that sense enemies and wars are not what they used to be. Arquilla and Ronfeldt argued that the information age has "offense-dominant attributes”. There has been an active debate in *Foreign Policy* between Thomas Rid and Arquilla on this subject, but there are many sceptics around, though the prospect of disabling or using for terrorist purposes any of the underpinnings of modern communications in war is alarming.

The famous ‘crime triangle’ sees all crime as the product of motivated offenders, situational opportunities, and capable guardians (including bystanders). In cybercrime and cyberwarfare, the level of capability is a matter of degree rather than a binary construct, and there are a lot of third parties in the private sector as well as the State who play an intervening role, even if – as Keith Alexander stated when defending his new roles in the private sector, he “didn't develop the idea while working at NSA, but even if he had, that agency lacks the authority to defend private networks. The agency mainly protects secret networks with classified tools and information sharing that does not exist in the private sector.” So strengthening the private sector as a national infrastructure goal presents some difficulties. But what is needed is to rethink the public private partnership role in a way that does not assume that the public sector holds the expertise and data, and the private sector are mere executives. These days, transnational businesses, including some private military companies, may have much that mere governments do not. We need to demystify ‘cyber’ a little, and emphasise the continuities as well as differences between crime, terrorism and warfare. Given that most MS have cybersecurity as tier 1 national security threats, NATO needs to focus on what it can do and needs to do to add value to individual MS efforts, and to sharing what is best – if individual MS are prepared to divulge it.

1. There is a common misrepresentation of ‘stolen’ in relation to secrets and identities. Normally if something is stolen, the victim no longer has it. However in such cases as identity and espionage, it is far more common that the victim simply no longer has exclusive ownership of themselves or their data. This may lead to feelings of invasion (if detected) and/or loss of economic value, but this is different from theft. [↑](#footnote-ref-1)