The reality and future of cyberwar

Myriam Dunn Cavelty

Conflicts in cyberspace are a reality: elements of any political, economic and military conflict now take place in and around the internet. Not surprisingly cyberwar has become a buzzword in the media and in the political debate. The term has come to refer to any phenomenon involving a deliberate disruptive or destructive use of computers. There also is a widespread tendency to hype the issue with rhetorical dramatization and alarmist warnings. True, cyber conflict might seem disconcerting and frightening, but the number one law in the cyberage is: don’t panic. The number two law: be precise in your use of language.

A conceptual distinction between different forms of conflict in cyberspace is necessary if we are to assess the risk and its possible consequences, to assign responsibility for addressing the conflict, but also to discuss the possibility and implementation of preventive and reactive countermeasures. Broad and imprecise use of the term cyberwar must be avoided — as should fear-based (over-)reactions.

Different forms of cyber conflict can be distinguished by focusing on the extent of damage and a cyber-escalation ladder can be built with rungs expressed by ‘severity of effects’. This helps policy-makers to prioritize: only computer attacks whose effects are sufficiently destructive or disruptive are an issue that needs to be addressed at the political level. Attacks that disrupt non-essential services, or that are mainly a costly nuisance, are not.

Cyber-escalation ladder

Rung one: cyber vandalism and ‘hacktivism’. This involves modification or destruction of content, such as the hacking of websites, or turning off a server by data overload. Hacktivism is the most common form of cyber conflict in tense political situations and receives much attention in the press. However, the effects of such actions are temporary and relatively harmless, even if it may be embarrassing for political institutions to be the visible victims of a cyber attack or if some (limited) economic damage results for companies with a strong internet presence.

Rung two and three: cyber crime and cyber espionage. In contrast to hacktivism, both take place all the time and independently of conflict. The main victim is the private sector. Even though collection of relevant data concerning damage is extremely difficult, the global cost of cyber crime was estimated at one trillion US dollars according to a study by McAfee, the internet security firm. Less common are entries into government networks containing classified information.

Rung four: Cyber terrorism. Consists of unlawful attacks against computers, networks, and the information they store. The aim of the attacks is to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack would result in physical violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered ‘cyber terrorism’. According to this definition, the world has yet to see an act of cyber terrorism.

Rung five: cyberwar. Refers to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. In military terms, such activities are known as Computer Network Attack (CNA), a concept which is part of the official information operations doctrine. Two types need to be distinguished: CNA as a tactical-operational means in the context of an overall operation or CNA as a strategic, stand-alone tool.

Such a narrow and precise definition not only helps to circumvent dangers inherent in calling something ‘war’, like exculpating the victims of an attack from their own responsibility for the consequences of their negligence in terms of computer security, or creating pressure to retaliate against ‘hackers’, real or imagined. It also helps when we want to address the reality of the phenomenon.
The other side of the coin: defensive measures

Every offensive concept is accompanied by a defensive counterpart: CNA is complemented by Computer Network Defense (CND). The truth is that the majority of countries attribute greater importance to defensive measures than to possible offensive operations. But the limits of military influence also become apparent rather quickly: CND is limited to military networks. Countermeasures on all rungs of the cyber-escalation ladder, be they preventive or reactive, are dominated by civil concepts. This is exactly how it should be, because measured by the number of actual incidents and the estimated extent of damage, cyber crime, and closely linked to it cyber espionage, are by far the most serious problems the world faces today.

In addition, when a particular detrimental event occurs, it is often impossible to determine in a timely manner whether it is the result of a malicious attack, a failure of a component, or an accident. Secondly, although their goals are different, in cyberspace the tools and tactics used by armies, terrorists, and criminals are the same. What category of the cyber-escalation ladder we are faced with therefore depends on the motivations of the attacker and the circumstances surrounding the attack. We can only categorize with certainty after investigating the incident. The law is the main reactive countermeasure.

Another countermeasure for the first three rungs of the ladder is ‘information assurance’, which is about ensuring confidentiality, integrity, and availability of information and information systems. Every citizen and every company is responsible for protecting themselves. The government’s role is to protect its own networks and to ensure as legislator that gaps in internet or cyber law are closed. Because actors in cyberspace act mostly internationally, co-operation with other states is also very important. Further up the ladder, critical infrastructure protection plays a key role. These protection plans require primarily a close partnership between government and industry as well as intensive co-operation between countries.

But how good are our defenses? Technically speaking, a totally secure network does not exist: incidents will always happen. How likely is it, therefore, that cyberwar will bring truly devastating destruction in the future?

Cyberwar as strategic form of war of the future?

Reports about CNA as a mission-supporting element are on the rise. A prominent example is the rumored US cyber attack in 2007 on the cellular phones and computers that insurgents in Iraq were using to plan roadside bombings. However, such reports should be taken with a grain of salt. First, most of them are based on rumours. Second, we do not know who has what kind of offensive resources. The indicators used by intelligence agencies for the determination of CNA capabilities such as doctrine, training, simulation and industrial co-operation provide doubtful results.

What is assumed is that countries that have the ability to develop cyber weapons will do so. This is based on the image of cyberwar as a fundamentally different kind of warfare: cheap, ‘clean’ (because a hostile country can be compelled to its knees from afar, without bloodshed) and less risky than other forms of armed conflict because the attacker can remain anonymous.

Such visions forget that the potential existence of these capabilities does not necessarily mean that they will be used. Even if the technology existed and could really be targeted specifically at enemy infrastructures, its use raises a mass of legal, ethical, but also strategic issues.

From the perspective of a democratic state, offensive cyberwar remains highly controversial. The target is the entire communication infrastructure of an opponent, military and civilian. As a result, it is no longer possible to draw a clear distinction between combatants and non-combatants. Uncertainties also exist as to when the use of computers as a weapon constitutes an indirect or direct form of military violence or whether the mere intrusion into computer networks by a state body counts as violation of the principle of non-intervention.
Strategically, many caveats remain. First, the build-up of offensive cyberwar capabilities is far from cheap. Second, it is controversial whether strategic cyberwar would actually bring the promised benefits: sophisticated cyber weapons would need to be a lot more powerful than the usual hacking tools to deliver ‘effect’ to a particular geographic conflict zone or enemy. We would need to see a qualitative leap in the ability to penetrate and manipulate information and communication technologies and to directly control aspects of the information infrastructure. Furthermore, our dependence, though already quite high, on computer networks would still have to substantially increase in order for cyberwar to be effective. Third, very strong arguments can be made for the overall strategic interest of the world’s big powers in developing and accepting internationally agreed norms on the non-use of cyberwar weapons. The most obvious reason is that the countries that are currently considering offensive cyberwar capabilities are also the most vulnerable to attacks due to their dependency on information infrastructure.

And there is another danger to be considered: uncontrollable blowback. Clearly, there is a disjunction between the technological and market realities of a globalised, interdependent, and networked world and the idea of using cyberwar tools. There are a number of ways in which computer network attacks could – and most likely would – ‘blow back’ on Western societies. First of all, repercussions could emerge directly through the interdependencies between various critical assets that characterize the environment. Second, blowback may be felt through the more intangible effect of undermined trust in cyberspace, with damaging repercussions for the global economy. In this sense, let us hope that cyberwar remains science fiction forever.

Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich and Lecturer in the Department of Social Sciences and Humanities at ETH Zurich, Switzerland. She is author of Cyber-Security and Threat Politics: US Efforts to Secure the Information Age; Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, (co-edited with Kristian Søby Kristensen); Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, Ashgate 2008 (co-edited with Victor Mauer and Sai-Felicia Krishna-Hensel).