Parliamentary **Assembly**
Assemblée parlementaire

Parliamentary Assembly
Assemblée parlementaire

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 11335
27 June 2007

How to prevent cybercrime against state institutions in member and observer states?

Opinion[1]
Political Affairs Committee
Rapporteur for Opinion: Mr Pedro AGRAMUNT, Spain, Group of the European People's Party

I. Conclusions of the Committee

1. The Political Affairs Committee fully supports the report by Mr Sasi, Rapporteur of the Committee on Legal Affairs and Human Rights. At this stage of the Information age, our societies depend on technology and are vulnerable to it:

- cyber-attacks are more and more frequent and sophisticated;
- many of them are politically-motivated and target government and military websites;
- they have the potential to disrupt the provision of essential services and prejudice the life and safety of ordinary citizens;
- their authors can be private individuals expressing their opposition towards the policy of a certain country and advancing their political agenda;
- so far it has never proved to be the case, but state-sponsored cyber-attacks are conceivable.

2. In this light, cyber-security should be a primary objective for our governments. This is not only a matter of economic crime but also of national security. It is time for this issue to come out of the realm of a few specialists and be debated at political level, as it implies a new approach to the way in which we conceive international relations, the relationship between states and private individuals and the threat of terrorism.

3. The Council of Europe can play a role in supporting the harmonisation of a legislative framework against cybercrime. The Assembly should, therefore, reiterate its call for the widest possible accession to relevant Council of Europe treaties, in particular, the Council of Europe Convention on the Prevention of Terrorism and the Convention on cybercrime

4. In developing a comprehensive strategy against cybercrime, states should find appropriate ways to involve private actors, such as computer, networking and software industries.

II. Amendments to the draft resolution proposed by the Committee

Amendment A:

Paragraph 2, replace: 'democracy, human rights, the rule of law, and that' with:

'democratic stability and national security, and raises fundamental issues as regards the respect of human rights and the rule of law. Thus,'

[1] See doc. 11325 tabled by the Committee on Legal Affairs and Human Rights.

Amendment B:

Paragraph 3, before ‘Indeed’, add the following sentence:

‘Politically-motivated attacks against military or government websites of a number of Council of Europe member and observer states are increasingly frequent and sophisticated.’

Amendment C:

Paragraph 4, at the end of the paragraph, add a new sentence:

‘This threat can emanate from private individuals, organised groups or states’.

Amendment D:

After paragraph 6, insert a new paragraph:

‘The Assembly also recalls that the Council of Europe Convention on the prevention of terrorism offers an additional instrument in the fight against cyber-terrorism, as well as against the use of the Internet for terrorist purposes.’

Amendment E:

Paragraph 7, replace ‘states have not yet ratified this important Convention’ with:

‘and observer states have not yet ratified these important Conventions’

Amendment F:

Paragraph 13, at the end of the paragraph add a new sentence:

‘In doing so, they should involve private actors, including computer, networking and software industries.’

Amendment G:

Paragraph 14, sub-paragraph 2, after ‘sign and ratify’, insert:

‘the Council of Europe Convention on the Prevention of Terrorism,‘

* * *

III. Explanatory memorandum, by Mr Pedro Agramunt, rapporteur for opinion

1. Introduction

1. In the Information age, our societies depend on technology and are vulnerable to it. At this point in time, the reconsideration of the traditional concepts of sovereignty, national security and war imposes itself, in the light of the fact that private individuals can paralyse the normal functioning of a state without even moving from their computer, wherever they are on the planet.

2. Cyber-attacks are not simply the deeds of a few young people who hack ‘for fun’, but can be a deliberate decision by some individuals to launch a politically-motivated attack against a state, to exert pressure on it and advance their political agenda or simply to retaliate against a policy with which they do not agree. Given the rapidity with which the information is shared on the Internet, it is not even necessary for them to be linked to a group long before the beginning of the cyber-attack: through social networks and blogs, unknown people from different countries can meet and unite behind the same political objective in a few minutes. Whether these individuals act spontaneously, or under the influence of a terrorist, criminal or other group, or the sponsorship of a state is an open question and the answer can vary from case to case. All three of these scenarios are possible.

3. In addition, nowadays automated attack tools are freely available on the Internet. As soon as the vulnerability of a particular operating system or application becomes public knowledge, the release on the Internet of tools exploiting that vulnerability takes place within a few hours. These *weapons,* therefore, are available to everybody.

4. This disruptive - and in the worst case, destructive – potential of private individuals should be taken very seriously by politicians because it can affect the safety of our citizens. As I will explain better in my Opinion, cybercrime is a matter of national security and defence. It is a matter of civil liberties and freedom of expression on the Internet, and their legitimate limitations. Furthermore, it is undoubtedly a matter for international cooperation, as hackers operate without borders, and gaps in the framework for the prevention and the criminalisation of hackers' activities in one country will have repercussions in others.

5. It was therefore high time that our Assembly devoted its attention to the issue of cybercrime with a comprehensive approach, involving the Political Affairs Committee and the Economic Affairs Committee in addition to the Committee of Legal Affairs and Human Rights. I would like to express my appreciation for Mr Kimmo Sasi’s excellent report and I congratulate him for taking the initiative of bringing the issue of cybercrime back on the Assembly’s agenda.

2. Forms of cyber-attacks

6. In most cases, cyber-attacks do not have a political but an economic motive, and are aimed at ill-prepared small to medium-size business, with poor defence capabilities. However, politically-motivated attacks do take place and include, amongst their most frequent targets, TV and radio channels, on-line newspapers and state-related websites.

7. Instead, the large and well-protected military and government networks require relatively greater time, skill and experience to penetrate. However, cyber-attacks are becoming more and more sophisticated and are also capable of hitting these sensitive websites. Amongst the main targets are the United States, China, Brazil, Australia, the United Kingdom and Turkey.[2]

8. The forms that cyber-attacks can take include:

- clandestine high-jacking of a system;
- denial of service;
- destruction or theft of sensitive information;
- breaking into a network;
- cracking of software protection; and
- phreaking (such as sabotage or high-jacking of telephone exchanges).

3. Politically-motivated cyber-attacks

9. Trends in cyber-attacks reflect political tensions worldwide. Since the mid-nineties, when information on this phenomenon started to be collected, it has been possible to notice a direct correlation between the breaking out of political crises and the frequency of cyber-attacks.

10. The recent cyber-attack against **Estonia** is only one of the most recent of these politically-motivated cyber-attacks. This attack was particularly virulent as it succeeded in shutting down the country's digital infrastructure; saturating the websites of the main state institutions and governmental agencies; staggering Hansabaka, Estonia's biggest bank; and overwhelming the sites of several daily newspapers. The attackers used a giant network of enslaved computers, spreading from North America to the Far East, to generate very large packets of information streams which produced denial-of-service attacks. The reason why this attack was so successful is that, for Estonia, the first critical infrastructure is the Internet itself: Estonia is one of the most Internet-connected countries in the world, where almost every single aspect of ordinary citizens' lives are managed by IT infrastructures.

[2] http://www.mi2g.com/.

11. There are clear indications that there was a link between the government's decision to relocate the Bronze Soldier statue from the Tallinn city centre, where it had stood for sixty years, to the war cemetery and the action of the hackers.[3]

12. There are many other examples of politically-motivated cyber-attacks, the most significant including:

- **the cyber-attack against NATO in April 1999**, following the beginning of NATO air strikes against Serbia: according to the statements of then NATO spokesperson, it seemed that some attackers in Belgrade opposing the bombings had hacked into the NATO website and caused line saturation of the server; they also infiltrated and clogged the defence alliance's computer system[4]; the following month, in retaliation to the accidental bombing of the Chinese Embassy in Belgrade by NATO, **Chinese hackers** have targeted US government websites;[5]
- since 2000, **Armenian and Azerbaijani websites** have been affected by several rounds of cyber-attacks motivated on the grounds of the Nagorno-Karabakh conflict;[6]
- the publication of the **Danish cartoons** of the Prophet Mohammed provoked a worldwide online campaign of protests against Denmark in February 2006. In particular, its targets were the newspaper that first published the cartoons, as well as other prominent Danish sites.[7]

4. A new form of warfare?

13. The possibility of large-scale digital warfare was envisioned and announced a long time ago by a number of think-tanks and security experts. Now the recent case of Estonia has led many to think that the time is ripe for this kind of war. This forces all those concerned, especially politicians, to redefine the very concept of warfare.

a) Private individuals waging war against states or state-sponsored attacks?

14. As I already mentioned, the cyber-attacks against Estonia were by private individuals acting out of political motives, whose action was triggered by the removal of the Bronze Soldier. Despite some initial suspicion and the huge financial effort to set up such a large-scale attack, it appears that the Russian authorities were not behind their actions. Of course, in a fictitious scenario it is also possible to conceive that behind a cyber-attack by a group of private individuals there might be the political orchestration by a state, but so far this has never proven to be the case. In fact, it is also possible to imagine situations where the citizens of a country decide to take a political position towards a foreign country which is not in line with their country's official policy, or for citizens to use cyber-attacks against their own country, as a means of political pressure.

15. In the Information age, war does not take place necessarily between states, but can have, as opponents, a group of private individuals and a state. The problem, for states, is how to devise an effective strategy to defend themselves against cyber-attacks, including those by non-state agents, namely:

- how to prevent them;
- how to mitigate their effects; and
- how to restore normality after an attack, within an acceptable time-frame and at an acceptable cost.

16. In devising a strategy, states should be aware not of:

- the need for international cooperation;

[3] http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598.
[4] Sci/Tech Kosovo info warfare spreads, BBC online, 1 April 1999.
[5] Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says, CNN online, 12 May 1999.
[6] Nagorno-Karabakh dispute takes to cyber space, www.eurasia.net, 8 February 2007.
[7] Muslim hackers hit 3,000 Danish websites, United Press International, 22 February 2006.

- the need for an appropriate and harmonised legal framework criminalising cybercrime; and
- the need to strike a balance between respect of civic liberties and fundamental rights and ensuring public security; but also of
- the need to involve public as well as private actors in this strategy, as the weakness of the protection system of the latter could have a considerable negative impact on the safety and security of ordinary citizens. Cooperation with computer, networking and software industries will be particularly important.

b) Cyber-attacks in the context of inter-state war

17. Inter-state war might also undergo transformations due to the use of digital technology: cyber-attacks could be employed to disrupt the enemy's communications or other key services, before or in conjunction with other military operations. As in all other matters concerning cyberspace, the United States of America has been a pioneer in foreseeing this kind of actions in its defence strategy.[8] It has even set up a team which is responsible for coordinating offensive computer network operations (the Joint Functional Component Command for Network Warfare, JFCC-WF)[9].

18. But it is not the only one: a US military report into the future of geo-political relations with China has claimed that the Chinese government is developing a cyber-warfare division for use in possible future conflicts.[10] Indeed, it is reasonable to wonder whether cyber-dominance is going to be the main feature of military power in the near future.

5. Use of the internet for terrorist purposes and cyber-terrorism

19. Terrorist networks have been making full use of the Internet right from its start and have proved to have remarkable experts in this field. They are versed in operational security and know how to mask their true geographical locations through proxy servers. Amongst the activities which they conduct via the Internet are:

- **recruitment, training and propaganda:** there are instructions on how to make bombs, web discussion fora calling for jihad, information on terrorist training-camps; even the planning of operations takes place on the Internet, through covert websites. In this respect, it should be mentioned that the 2005 Council of Europe Convention on the Prevention of Terrorism establishes as criminal offences acts that might lead to the commission of acts of terrorism, including public provocation or indirect incitement, recruitment and training for terrorist purposes, apology of terrorism, etc.[11]

- **Retrieval of sensitive information:** it is not uncommon for information about critical infrastructure to be ferreted via the Internet. After research by security services, attacks of this kind in 2002 were traced back to IP addresses in Indonesia, Kuwait, Pakistan and Saudi Arabia. Sophisticated computer programmes used by engineers to find stress points and weaknesses in buildings, bridges and dams were also found in 2001 and 2002 in computers belonging to Al-Qaeda members in Afghanistan.[12]

20. By **cyber-terrorism**, however, it is meant that terrorists target the Internet and electronic communication. This represents a real threat, in itself or if used in conjunction with other kinds of attack: it is possible to imagine digital attacks that cripple emergency response, transport or communications, in order to magnify the impact of a physical attack.

[8] The White House, The National Strategy to Secure Cyberspace, February 2003; US ponders cyber war plans, BBC online, 7 February 2003; Pentagon plans cyber-insect army, BBC online, 16 March 2006.

[9] U.S. Military's Elite Hacker Crew, www.wired.com, 18 April 2005; see also: http://www.stratcom.mil/organization-fnc_comp.html.

[10] Department of Defence of the United States, Annual Report to Congress, The Military Power of the People's Republic of China, 2007.

[11] As of today, this Convention, which is open to non-member states for accession, has been signed by 39 member states and ratified by 7. A further 10 countries are completing their domestic process leading to ratification.

[12] http://www.mi2g.com/

Reporting committee: Committee on Legal Affairs and Human Rights

Committee for opinion: Political Affairs Committee

Reference to committee: Request for urgent debate, reference No. 3365 of 25 June 2007

Opinion approved by the committee on 27 June 2007

Secretariat of the committee: Mr Perin, Ms Nachilo, Mr Chevtchenko, Mrs Sirtori-Milner, Ms Pieter, Mr Alarcon