

**CYBER-CRIME AND CYBER-WAR :**  
**THE MILITARISATION OF THE FIGHT OF CYBER-CRIMINALITY**

Benoit Gagnon  
(Encadré par Stéphane Leman-Langlois)

*European Society of Criminology*  
*Edimbourg (Ecosse), 2-5 septembre 2008*

---

February 2000. A hacker is launching a series of highly publicized denial-of-service cyber attacks against large commercial websites including Yahoo!, Amazon.com, Dell, Inc., E\*TRADE, eBay, and CNN. Hacker's codename: Mafiaboy. The US Federal Bureau of Investigation (FBI) and the Royal Canadian Mounted Police (RCMP) acted quickly after they intercepted a discussion in a Internet Relay Chat (IRC) chat room where one person claimed responsibility for the hack. They finally arrested a 16 years old boy in April 2000.

May 2007. The Estonian government is targeted by a massive denial-of-service attack after a monument honoring Russian World War II dead is moved amidst intense opposition from the Russian ethnic minority. Responsibility for the DDoS is attributed to Russian hackers. As the government's networks are literally submerged with bits of information, the economy begins to suffer from the resulting paralysis of its web-based activities. Eventually, the Estonian government, having exhausted its own capabilities, officially requests NATO's help in defending its computer infrastructure against the continuing cyber attacks. Russia is identified as the most probable origin of the cyberattack. Although the Russian government is not officially accused of launching, participating in or facilitating it, Silver Meikar, a Member of Parliament in the governing coalition, who follows information technology issues in Estonia, tells the press that "there are strong indications of Russian state involvement. I can say that based on a wide range of conversations with people in the security agencies". Instant media frenzy was thus created, and experts quickly identify the Estonia-Russia incident as "the first cyberwar".

The two events are not linked, but both tell us a lot about the structure and deployment of various cybersecurity agencies. In the first case, police agencies acted on behalf of the state to respond to the perpetration of a cybercrime. In the second case, military organizations were mobilized to respond to an act of cyberwar — by using tactics akin to cybercrime.

This presentation has two objectives. First, we are going to show that a militarization of the fight against cybercriminality is currently taking place. A description of current trends in cybersecurity will demonstrate that the mindset of cybersecurity agencies is clearly a "national security" mindset, in which military or military-like institutions are asked to play a key role. Second, we will describe how cybersecurity agencies are, on one hand, fighting cybercrime and prosecuting their authors while planning and committing cybercrimes themselves. One common example is the use of network-enabled attacks against other countries or against their own citizens justified by "raison d'État". This paradox is quite common in the cybersecurity discourse held in various levels of government, in which the recourse to criminal tactics is justified when protecting national cybersecurity.