

**The proliferation of cyber security strategies  
and their implications for privacy**

**Benoit Dupont**

Canada Research Chair in Security and Technology  
Université de Montréal

[benoit.dupont@umontreal.ca](mailto:benoit.dupont@umontreal.ca)

**Published in:**

Karim Benyekhlef and Esther Mitjans (eds.), *Circulation internationale de l'information  
et sécurité*, Les Éditions Thémis, Montréal, pp. 67-80, 2013.

The commercial internet has now been in existence for almost fifteen years, but it seems that Western government have barely realized the extent to which this technology is redefining security issues, and are scrambling to design policies specifically addressing this new class of risks. Until then, the folklore associated with computer hackers and their supposed ability to launch a nuclear war from their parents' basement or to bankrupt the whole financial system remained mostly a Hollywood myth<sup>1</sup>. Although the spectre of cyber-terrorism was raised at regular intervals in the late 90s and early 2000s by some scholars (Denning, 2000), the event of 9/11 and following attacks in Madrid, London or Bali, to name a few, clearly demonstrated that none of the existing terrorist groups realistically considered that computers could generate the same amount of terror among their opponents than crudely assembled explosive devices detonated in public areas by suicide bombers. Of course, I am not arguing that governments have been idle over the years. On the contrary, they developed technical and investigative capacities that were responsible for some high profile hackers' arrests and managed to shut down underground criminal online markets through the use of creative infiltration strategies (see for example Poulsen, 2011). Computer emergency response teams have also benefited from the institutional support of various government agencies. But this approach was fragmented at best, and it was only very recently that the internet captured the attention of national security policy makers, leading to the proliferation of national cybersecurity strategies (CSS) that rely on a more integrated 'whole of government' approach. Their stated objectives are to more systematically address the diversity of risks associated with the embeddedness of this recent technology into every aspect of our lives, from the daily operations of key infrastructures to the flow of transactions that irrigate our financial system and the personal communication tools that sustain our social interactions. Hence, this short contribution will examine the common features that seem to define these CSS, from the way they frame the risks they seek to protect us from, to the specific initiatives they advocate and the financial and institutional resources they plan to mobilize in the process. I will also discuss what is not included in these strategies, as what is deliberately left unsaid or kept very vague can highlight the decisions that were made, and therefore the alternatives that were discarded. The potential implications these CSS will have on online privacy will also be discussed in a final section, where I will argue that privacy advocates have underestimated the disruptive role CSS might play in framing a new internet regulatory regime mainly defined through security.

## **The compressed chronology of cybersecurity strategies**

Before launching into an overview of these CSS' content, a brief description of their recent history is required in order to understand in what context they were drafted. One of the earliest documents that could qualify as a CSS is Presidential Decision Directive 63,

---

<sup>1</sup> See for example Wargames (1983), Sneakers (1992), Hackers (1995), Swordfish (2001), Die Hard 4 (2007), etc...

issued in May 1998 by the White House (1998). On the eve of the new millennium and the threat of catastrophic disruptions caused by the Y2K bug, the US government acknowledged the dependence of its economy and critical infrastructures upon “cyber-based information systems”. In order to limit the exposure to this perceived new vulnerability and to reinforce the government’s capacity to respond to computer and physical attacks, new coordinating mechanisms and planning arrangements were designed, with a strong emphasis on public-private partnerships. This template was updated in 2003 and published as the National Strategy to Secure Cyberspace. The newly created Department of Homeland Security (2003a) became responsible for its coordination and implementation. Although critical infrastructure protection is still mentioned in this strategy’s objectives, the threat focus is instead designated in this document as “cyberspace”, which is defined as “the nervous system [of critical infrastructures] composed of hundreds of thousands of interconnected computers, servers, routers, switches and fibre optic cables” (DHS 2003a: vii). The physical protection of critical infrastructures was addressed in a separate document released at the same time (DHS 2003b). The private sector retains a central role in the strategy, although its participation is purely voluntary. Indeed, the strategy formally rejects regulatory tools as a primary mean to secure cyberspace, stating that “*the market itself is expected to provide the major impetus to improve cybersecurity*” (DHS 2003a: 15). The election of President Obama in 2008 did not significantly alter the efforts that had been launched by his predecessor, George W Bush, in order to enhance the US government’s capacities to defend its interests against online threats, it just made them more transparent (White House 2010). Known as the Comprehensive National Cybersecurity Initiative, this strategy increased the number of technical measures implemented to decrease the risks of intrusions and attacks against government networks, and called for improved information sharing between various agencies and external stakeholders.

The year 2008 also marked the end of the monopoly exercised by the US government on CSS. In May, Australia publicized a four year cybersafety plan that was quickly followed by a proliferation of CSS coming from other countries. The table below summarizes the date, country of origin, name and, if available, the responsible government department for each of these strategies.

<b>Date</b>	<b>Country</b>	<b>Name</b>	<b>Department responsible</b>
May 1998	USA	PDD 63	White House
Feb. 2003	USA	National Strategy to Secure Cyberspace	Department of Homeland Security
Jan. 2008*	USA	Comprehensive National Cybersecurity Initiative (CNCI)	White House

May 2008	Australia	Cybersafety Plan	Department of Broadband, Communications and the Digital Economy
June 2009	UK	Cyber Security Strategy of the United Kingdom	Cabinet Office (Prime Minister)
Dec. 2009	Australia	Cybersecurity strategy	Attorney General's Department
Oct. 2010	UK	Strategic Defense and Security Review	Cabinet Office (Prime Minister)
Oct. 2010	Canada	National Cybersecurity Strategy	Ministry of Public Safety
Feb. 2011	France	French strategy for the defense and security of information systems	ANSSI (National Information Systems Security Agency)
Feb. 2011	Netherlands	National Cyber Security Strategy	Ministry of Security and Justice
March 2011	Germany	Cyber-security strategy for Germany	Federal Ministry of Interior
May 2011	USA	International Strategy for Cyberspace	White House
June 2011	New Zealand	Cyber security strategy	Ministry of Economic Development
July 2011	USA	Strategy for Operating in Cyberspace	Department of Defense

\* Released publicly in March 2010.

This list is certainly not exhaustive, and more strategies are to come, as the International Telecommunication Union (ITU) published in September 2011 a National Cybersecurity Strategy Guide (Wamala, 2011) offering guidelines to countries that have limited policy capacities in this domain. A few preliminary comments can be made however. First, although CSS usually involve a broad range of governmental agencies, the level of the “lead” or coordinating institution varies greatly from one country to another. In the US and the UK, the ownership of such policies is assumed by the highest political authority (the president and the prime minister), while in Australia, Germany, New Zealand or Canada, this task is delegated to a minister, indicating perhaps that the issue of cybersecurity does not rank as high on the agenda. In France, the specialized agency in charge seems even more peripheral, even if it is technically placed under the responsibility of the prime minister and his secretary general for national defence. For countries that are coordinating their cybersecurity efforts at the ministerial level, the choice of a law enforcement/justice authority (Australia, Germany, Canada) instead of an economic/communications focus (Australia initially, New Zealand) also suggests the existence of different approaches toward this new class of risks. Finally, the budgets allocated to various CSS – when they are made public and when they reflect additional resources instead of a simple reshuffle of existing programs, allow us to crudely assess the real commitment of governments, beyond high profile announcements. Because these

policies span multiple budget lines and they have started to appear in the middle of one of the worst economic recessions of the last two centuries, reliable numbers are still scarce. However, one can speculate that the billion CAD dollars set aside in new funding over four years by the UK government for cybersecurity in its Strategic Defense and Security Review indicates a high priority, while the more modest pledges made by countries such as Australia (126 million dollars over four years) or Canada (90 million dollars over five years) reflects a more cautious approach. By comparison, the 3.2 billion US dollars budgeted by the Pentagon for the 2012 Fiscal Year and the 769 million US dollars requested by the White House for cybersecurity programs at the Department of Homeland Security for the 2013 Fiscal Year indicate the resolve of the US government to retain a technological dominance over the digital realm (Zorz, 2012).

### **The curiously similar content of cybersecurity strategies**

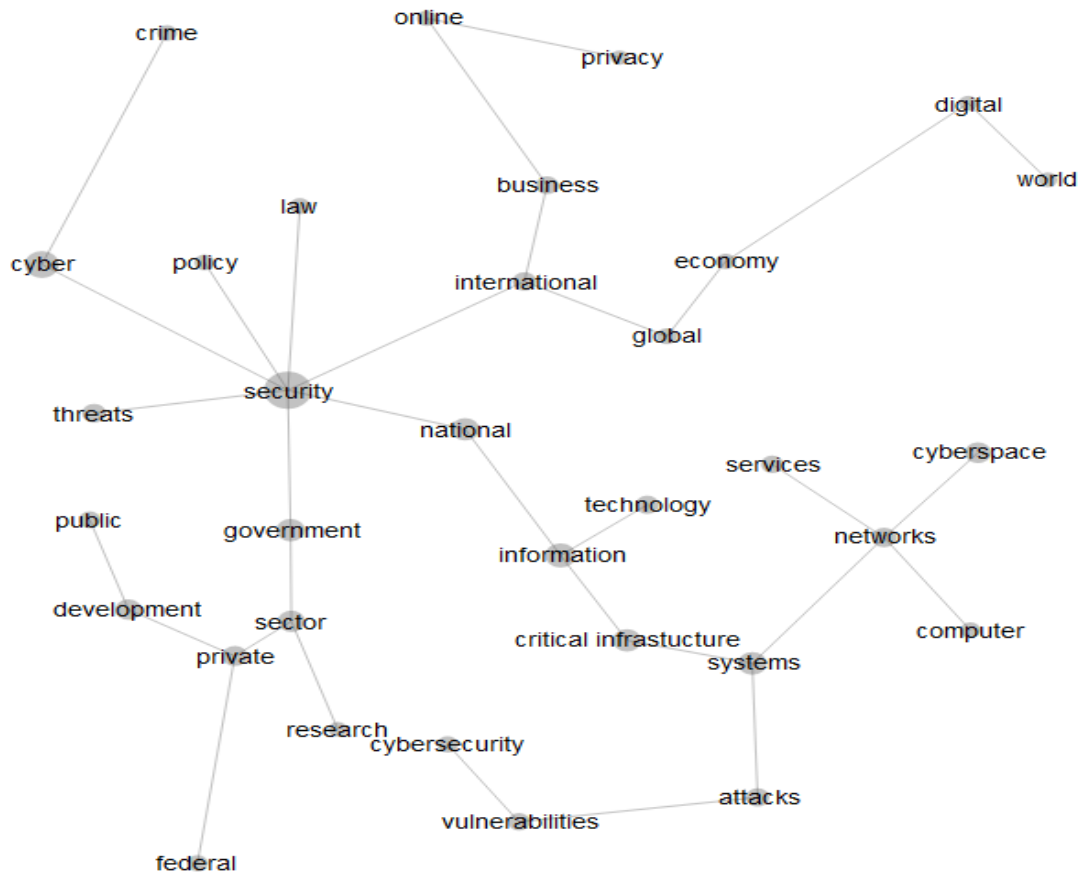
Beyond the timing and institutional context in which these CSS were formulated and adopted, their content also provides us with some invaluable information about their underlying rationale, and by extension on the tangible programs and measures that will come out of them. Eleven of the fourteen documents listed on pages two and three<sup>2</sup> were retrieved from the internet and fed into Leximancer, an automated text analysis software that applies machine-learning techniques to huge quantities of documents and “*learns in a grounded fashion what the main concepts in a corpus are and how they relate to each other*” (Rooney, 2005). The concept map below illustrates how the 33 main concepts identified by the software from the 46,403 words it analyzed are clustered and connected to each other.

What strikes the reader when all these documents are examined together, besides the fact that most of them are extremely short and concise (considering the complexity of the problems to solve), is their level of similarity. From the examples that are used to make the risks more explicit and vivid, to the responses that are outlined, down to the iconography appearing on their covers to represent online threats and potential victims. Indeed, if sections were to be pulled out from these strategies and presented to an educated audience of cybersecurity specialists, it would probably be difficult for them to tell from which country they originate. The magical global recipe that seems to fit all sizes and needs revolves around four main “ingredients”, which are or course strongly interconnected.

---

<sup>2</sup> The three documents that were not included in the analysis are PDD 63 and the National Strategy to Secure Cyberspace from the USA, as well as the Australian Cybersafety Plan, for which not policy document could be found beyond a press release and a promotional web page.

**Figure 1. Concept map drawn by Leximancer from eleven cybersecurity strategies**






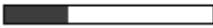




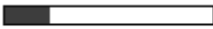

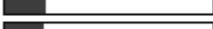

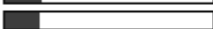

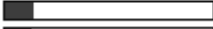



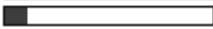




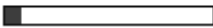
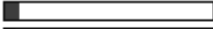




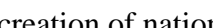
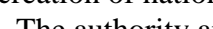


### 1. Better protection of critical infrastructures

The first element, which appeared as the main justification for the release of the precursor PDD 63 document, insists on the need to considerably reinforce the digital security of critical infrastructures. New technical norms and standards reflecting a stronger level of state intervention are called for, and some CSS even mention several technological platforms under development or at an early deployment stage, whose specific aims are to reinforce the protection of existing infrastructures. The CNCI (White House, 2010) explains for example how the EINSTEIN 2 and 3 tools will be able to detect and prevent intrusions inside government systems. The US Department of Defense also mentions in its own CSS the Defense Industrial Base cyber pilot launched in June 2011, where defense contractors and their internet service providers are offered filtering tools designed by the National Security Agency to analyse incoming traffic and prevent malicious attacks (DoD, 2011: 8). The subtext of this focus on critical infrastructure suggests that we are currently vulnerable to cyber attacks from an undefined enemy and that we must considerably reinforce our state of readiness against such looming threats. Such a catastrophic scenario and its disastrous outcomes are promoted as a credible alternative in many CSS, despite the fact that such attacks have never been recorded to

date, and would probably be detected and stopped before they could reach a systemic level. Although improving the computer security of critical infrastructures is a legitimate goal in itself, the fear-mongering tactics used to justify such approaches appear so exaggerated that they might prove counterproductive. By contrast, when the main concepts found by Leximancer are ranked by decreasing order of importance (see Table 1 below), it appears that the much more common phenomenon of cybercrime and computer fraud barely scores one third of the mentions relating to critical infrastructure threats (126 blocks of text containing the concept of crime versus 347 blocks of text discussing critical infrastructures).

**Table 1. Cybersecurity strategies' concept ranking**

Word-Like	Count	Relevance	
security	1129	100%	
cyber	684	61%	
information	450	40%	
systems	388	34%	
cyberspace	370	33%	
government	360	32%	
national	352	31%	
critical	347	31%	
development	319	28%	
sector	287	25%	
networks	256	23%	
attacks	256	23%	
threats	247	22%	
private	241	21%	
international	229	20%	
business	214	19%	
technology	200	18%	
vulnerabilities	192	17%	
services	186	16%	
public	161	14%	
federal	149	13%	
cybersecurity	136	12%	
law	129	11%	
crime	126	11%	
computer	121	11%	
online	118	10%	
policy	116	10%	
global	107	09%	
digital	96	09%	
economy	93	08%	
world	86	08%	
research	75	07%	
privacy	57	05%	

## 2. National coordination mechanisms

A second recurring theme found in CSS involves the creation of national coordination mechanisms, both at the policy and operational levels. The authority and responsibilities allocated to these new positions and agencies will extend over a broad range of government stakeholders such as defence, public safety, industry, foreign affairs or even education ministries. We have already noted how different ministries dominate the conversation in various countries, and how these choices are likely to influence the leadership styles and the implementation of specific CSS. It would not be surprising for example to find that countries which favour industry and communications ministries to

lead their efforts rely more heavily on responsive regulatory strategies and public-private partnerships than governments where military and law enforcement institutions have prevailed. Obviously, the laudable intent is to avoid duplication and to adopt a whole-of-government approach destined to increase capacities and reduce waste. Yet, the conflicting rationalities that characterize these agencies (not to mention the turf wars that will inevitably arise) do not seem to concern the designers of these strategies. To what extent is the secrecy required by intelligence agencies such as the National Security Agency or the Canadian Communications Security Establishment compatible with the definitely more transparent and consultative ethos of industry and economic ministries? Published CSS do not acknowledge these challenges and do not clarify how these contested rationalities will be arbitrated.

### 3. Partnerships with the private sector

As the backbone of the internet is operated by private interests, and several corporations such as Google, Facebook or Microsoft control a disproportionate share of online traffic, most CSS insist on the importance of building strong partnerships with a broad range of private actors. What is rarely specified is what governance and accountability mechanisms are planned in order to ensure that these partnerships are not transformed into informal tools of massive surveillance, as it would be very tempting (some would say almost irresistible) for law enforcement and intelligence agencies to circumvent cumbersome traditional court orders via euphemistically-called “information-sharing” agreements in order to access troves of personal data.

### 4. International cooperation

Finally, the global scale of the cybersecurity problem is addressed through systematic calls for stronger international cooperation. But this approach is mainly restricted to a limited number of allies from the Western world, and there are very few considerations on how to engage countries with emerging economies or even developing countries, which are often accused of being the causes of online insecurity.

In other words, the statements found in these strategies are fairly general in nature and filled with virtuous intentions such as calls for better coordination, more intensive international cooperation, enhanced information sharing, etc., but very little specific details are being offered to explain how these strategies will be effectively implemented and how their success will be assessed. CSS recycle a classical policy toolbox that sorely lacks in innovation and creativity, relying on 20<sup>th</sup> Century institutional arrangements to address problems of the 21<sup>st</sup> Century. Furthermore, the offensive capabilities being developed by most Western countries are barely discussed in their CSS, overlooking a very significant source of risks. To illustrate this point, it is ironic that the computer worm Stuxnet is mentioned as a justification for decisive action against these hostile but unspecified threats in the German and Dutch CSS, while the consensus among computer security professionals seems to be that this virus was created by US and Israeli intelligence agencies to cripple the Iranian nuclear programme (Broad et al., 2011).



## **Implications for privacy and the rule of law**

One way to measure the role privacy plays in these CSS is to quantify the frequency with which the concept appears in the eleven documents. Table 1, presented on page five of this document, shows that privacy comes last with a count of 57 and a relevance of 5%, meaning that blocks of text containing the term privacy appear twenty times less often than the most dominant concept, which unsurprisingly enough is security (count of 1129 and relevance of 100%). Clearly, security trumps privacy on a massive scale and the latter seems to play no more than a token role in these policies.

A major factor contributing to the marginalization of privacy is, in my opinion, the lack of evidence driving CSS. None of the documents analyzed for this contribution were able to estimate with an acceptable degree of confidence the scope of the cybersecurity problem. Most of them remain fairly general in their statements, and a few refer to dubious data generated by private sector service providers with a vested interest in exaggerating the threat. As a result, it will be difficult, if not impossible, to identify clear and reachable goals allowing us to know if these strategies are succeeding or failing. This is not a peripheral question, as governments are on the verge of spending billions of dollars to purchase new security products and services, mainly from the private sector, which will certainly have a negative impact on privacy. The lack of hard data also empowers prophets of doom who justify the erosion of privacy rights in the name of an impending digital Armageddon.

Privacy is also threatened by a dangerous confusion found in most CSS between four different kinds of (very real) risks that have very little in common:

- criminal risks (such as online financial fraud, cyberbullying, the production and exchange of digital child pornography, etc) that are the responsibility of law enforcement agencies and the courts;
- economic risks associated with the illegal download of intellectual property and protected contents, which mainly involve the entertainment industry and regulatory agencies (even if some countries have attempted to criminalize these risks);
- intelligence risks that involve private and public entities using the internet to acquire secrets from their competitors or adversaries;
- military risks that result in the destruction or incapacitation of digital and physical assets, and extend the domain of traditional armed conflicts to computer systems.

What is flawed in this unified approach is that it fails to acknowledge and to leverage the diversity of regulatory frameworks and capacities required to respond effectively to each specific type of risks. In this emerging framework, chances are high that the national security rationality will rule out more benign (and effective) forms of control, which is alarming from a privacy perspective.

Defence contractors, which will have to find new sources of revenues following the end of the Irak war and the planned withdrawal of coalition troops from Afghanistan, have noticed this new opportunity (some conspiracy theorists would certainly argue that they have actively contributed to shape it) and are taking active steps to colonize this new commercial space and play a central role in internet regulation. In Canada for example, the global IT firm CGI announced in October 2011 that it would launch a cyber-security unit located in Ottawa, whose vice-president will be a retired Lt General from the Canadian Air Force<sup>3</sup>. In the United States, the military-industrial complex is diversifying its offerings: BAE Systems, Boeing, L-3 Communications, Lockheed Martin, Northrop Grumman, Raytheon or SAIC have all launched their own cybersecurity solutions and are competing for a worldwide market that some analysts believe amounts to 80 to 140 billion dollars per year (Wolf, 2010).

Finally, the formulation process of CSS and their implementation did not follow a very transparent and deliberative approach. As a result, privacy advocates have not fully grasped how these new strategies will shape internet governance, technical and regulatory mechanisms in the name of security. While search and social media giants such as Google and Facebook certainly deserve to be kept in check, the emerging cyber-industrial complex (Brito and Watkins, 2011) that will support and implement these cybersecurity strategies certainly require all our attention, if we wish to protect the idea of privacy as it is currently understood.

---

<sup>3</sup> The CGI press release can be downloaded here: <http://www.cgi.com/en/CGI-appoints-IT-security-leader-Ken-Taylor-head-national-cybersecurity-practice>.

## References

---

- Brito, J. and T. Watkins (2011), "Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy", *Harvard Law School National Security Journal*, 3(1), pp. 39-84.
- Broad, W., Markoff, J. and D. Sanger (2011), "Israeli test on worm called crucial in Iran nuclear delay", *The New York Times*, January 16, A1.
- Denning, D. (2000), *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism*, US House of Representatives, May 23, Washington DC, available online at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>, last accessed on March 1<sup>st</sup>, 2012.
- Department of Defense (DoD) (2011), *Strategy for operating in cyberspace*, DoD: Washington DC.
- Department of Homeland Security (DHS) (2003a), *The National Strategy to Secure Cyberspace*, DHS: Washington DC.
- Department of Homeland Security (DHS) (2003b), *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, DHS: Washington DC.
- Poulsen, K. (2011), *Kingpin: How one hacker took over the billion-dollar cybercrime underground*, Crown Publishing: New York.
- Rooney, D. (2005), "Knowledge, economy, technology and society: The politics of discourse", *Telematics and Informatics*, 22(4), pp. 405-422.
- Wamala, F. (2011), *The ITU national cybersecurity strategy guide*, ITU: Geneva.
- White House (1998), *The Clinton administration's policy on critical infrastructure protection: Presidential Decision Directive 63*, May 22, Washington DC, available online at <http://www.fas.org/irp/offdocs/paper598.htm>, last accessed on February 22<sup>nd</sup>, 2012.
- White House (2010), *The Comprehensive National Cybersecurity Initiative*, Washington DC, available online at <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>, last accessed on February 22<sup>nd</sup>, 2012.
- Wolf, J. (2010), *Pentagon seeks tight ties with cyber contractors*, Reuters: Washington DC, available online at <http://www.reuters.com/article/2010/10/21/us-usa-cyber-pentagon-idUSTRE69J4OW20101021>, last accessed on February 29<sup>th</sup>, 2012.
- Zorz, Z. (2012), "The escalating costs of US cybersecurity plans", *Help Net Security*, 15 February, available online at [http://www.net-security.org/secworld.php?id=12411&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=12411&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29), last accessed on March 1<sup>st</sup>, 2012.