CEPS COMMENTARY
30 years CEPS
Thinking ahead for Europe

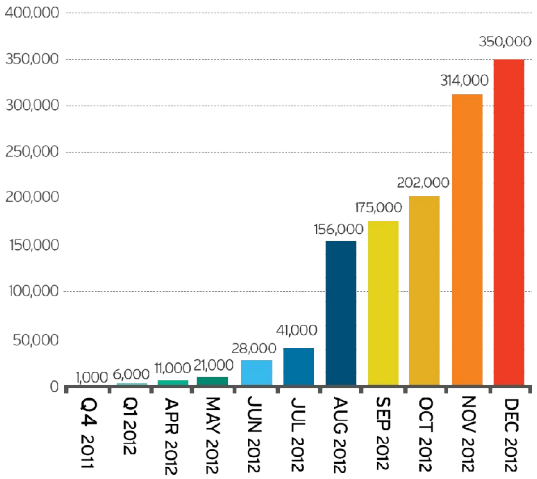
# The puzzle in the bits:
## Cybersecurity, digital warfare and the future of Internet governance

Andrea Renda

26 June 2013

The past year marked the rise of cybersecurity as the 'number one concern' for major economies, and monopolised the spotlight in recent talks between G2 Presidents Obama and Xi Jinping. Reports show that cyberattacks can easily target personally identifiable data, such as credit cards or healthcare information – as easily as the US Department of Justice or Iranian Nuclear facilities. Cyber threat is rising just as the Internet becomes a critical infrastructure for the global economy, with hundreds of new functions migrating to the network, and thousands more waiting to be hosted on cloud platforms, remote storage centres, smart grid management systems and machine-to-machine communication. Between April and December 2012, the types of threats detected on the Google Android platform increased by more than 30 times from 11,000 to 350,000, and are expected to reach one million in 2003, according to security company Trend Micro (see Figure 1). Put simply, as the global economy relies more on the Internet, the latter becomes increasingly insidious. It is efficient, no doubt: but is it also secure?

*Figure 1. Threats detected on Android platforms, March-December 2012*




*Source*: Trend Micro (2013).

Andrea Renda is Associate Senior Research Fellow at CEPS. This commentary is based on his Expert Brief entitled "Cybersecurity and Internet Governance", published by the Council of Councils, an initiative of the Council on Foreign Relations, published 3 May 2013 (http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621).

## The rise of the digital cold war

What's more, cyber-threats and cyber-attacks also hide an escalating 'digital cold war'. The United States has long been denouncing that the bulk of cyber-attacks that hit its institutions and companies every day are state-sponsored, and mostly China-sponsored or Iran-sponsored. Attacks are taking all forms, including massive penetration of the US market by cheap, often state-subsidised tech giants such as Huawei or Lenovo: the US imports almost $130 billion of high-tech products from China every year.[1] A recent, controversial report by security firm Mandiant documents the cyber-espionage campaigns conducted in recent years by a hacker group known as the 'Comment Crew' against more than 100 companies and organisations from different industries (the most attacked being IT), and observes that a secret Chinese military unit based in Shanghai was the most likely driving force behind a series of hacking attacks on the US. Not surprisingly, the new US spending law passed by Congress on 27 March 2013 prohibits any form of procurement of Chinese hardware in US institutions such as NASA, the Department of Justice and the Department of Commerce, unless a thorough assessment of "cyber-espionage or sabotage" risk by specialised federal officials has been carried out. Such assessment must include "any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized" by China. Tensions between Barack Obama and Xi Jinping over the rise of cyber-espionage has reached a peak in the past weeks: the US president has publicly stated that several attacks that have recently hit large banks, institutions and companies were "state sponsored", and made direct reference to China. On the other hand, Chinese experts claim to be the main target of state-sponsored attacks, mostly coming from the US. Table 1 shows that Russia and Germany have been the most frequent sources of cyber-attacks in March 2013, followed by Taiwan and the United States.

*Table 1. Source, number and type of attacks, March 2013*

Top 15 of Source Countries (Last month)

| Source of Attack | Number of Attacks |
|---|---|
| Russian Federation | 2,450,063 |
| Germany | 1,312,865 |
| Taiwan, Province of China | 537,738 |
| United States | 450,931 |
| Australia | 379,910 |
| India | 361,148 |
| Ukraine | 256,047 |
| Hungary | 237,778 |
| Brazil | 220,515 |
| China | 197,166 |
| Italy | 194,981 |
| France | 184,075 |
| Argentina | 183,093 |
| Japan | 151,861 |
| Venezuela, Bolivarian Republic of | 127,862 |

Top 5 of Attack Types (Last month)

| Description | Number of Attacks |
|---|---|
| Attack on SMB protocol | 6,163,431 |
| Attack on Port 5353 | 564,858 |
| Attack on SSH protocol | 383,315 |
| Attack on Port 17500 | 286,579 |
| Attack on Netbios protocol | 256,071 |

*Source*: Deutsche Telekom Cyber initiative.

[1] See W.M. Morrison (2012), "China-US trade issues", Congressional Research Service Report, 22 May 2012 (http://www.fas.org/sgp/crs/row/RL33536.pdf).

## What's happening to the Internet?

Originally created as a 'dumb' network, with intelligence distributed at the edges rather than at the centre, the Internet has always been a difficult place for policy-makers wishing to enforce the laws of the 'real world'. Already in the late 1990s, Carol Rose defined it as like "Central Park after dark", a place of both excitement and danger. And some authors did not hesitate to declare that some laws, including copyright, had no future in the Internet. The infancy of the Web saw the prevalence of freedom and neutrality over law enforcement and traffic filtering: law authorities have been chasing 'techies' and 'hackers'for years, but never gave the impression to be winning the war. The threat of Distributed Denial of Service (DDoS) attacks became a reality as early as 2001, when post-bubble IT companies such as Amazon, eBay, Yahoo! were severely hit. So, this is nothing new: the problem is that the stakes are becoming higher, as the Internet and, more generally, the IT environment increasingly permeates our lives. Already in 2004, the British Columbia Institute of Technology reported a ten-fold increase since 2000 in malicious attacks on process control systems, affecting critical services such as power utilities, sewage systems and wireless networks. In a few years from now, we will likely delegate to the IT infrastructure almost everything, from electricity consumption to tax declaration, and almost everything we do at work. Suffice it to think about 'smart cities' and 'machine-to-machine communications', which will lead to interconnecting everything from buildings to trains, dishwashers and smartphones, all governed by a conundrum of hardware and software located somewhere in a cloud. And what's more, in cyberspace, attack seems to always have a structural lead over defence, given that it is sometimes prohibitively difficult to foresee where, how, when attackers will launch their threat. Modern botnets apparently guarantee the result: within a given timeframe, any target can be attacked and damaged.

This is why our global community faces a tragic dilemma today. On the one hand, the neutrality of the Internet has proven to be a formidable ally of democracy and freedom: suffice it to think about the role of social networks during the Arab uprisings, or the work of bloggers such as Sana Saleem or Yoani Sanchez in otherwise heavily filtered countries (in their case, Pakistan and Cuba). This means that allowing too much traffic filtering might mean killing freedom of expression, by means of killing the end-to-end architecture that has made cyberspace an unprecedented forum for democracy. On the other hand, the cost of preserving users' freedom is skyrocketing every day: the US seems ready to abandon established privacy rights in the name of enhanced security, and the recent PRISM scandal confirms this sweeping impression. Key services such as e-commerce, e-health, e-government, M2M and tele-work might never take off if users aren't able to operate in a more trusted environment. And to be sure, some governments simply do not like ideas to circulate freely. A recent report by The Economist has shed light on the enormous amount of resources China is devoting to building a "giant cage", i.e. a domestic version of the Internet that allows for certain freedom to end users (such as opening microblogs), but with heavy automatic and even manual filtering of content by an army of civil servants. Countries like Pakistan and Kazakhstan have created huge national firewalls to ensure that people are limited in their behaviour. Recently elected Venezuelan president Maduro reportedly switched off the Internet for a few hours the day of the elections, to avoid easy reporting of illegal counting of votes. But even Mr. Obama has been given a new button to switch off the Internet back in 2009.

The question becomes more urgent every day: should the Internet remain an end-to-end, neutral environment, or should we sacrifice Internet freedom on the altar of enhanced

security? The answer to this question requires a brief explanation of how the Internet is governed today, and what might change in the future.

## The end of the Web as we know it?

Since its early days, the Internet has been left largely unregulated by public authorities (starting with the US 1996 Telecommunications Act), becoming a matter for private, self-regulation by engineers and experts, who have for years taken key decisions about Internet governance through rather unstructured procedures. No doubt, this has worked in the first years. As cyberspace started to boom, the stakes started to rise: rather informal bodies such as ICANN, a private multi-stakeholder association benevolently supervised by the US government that rules on domain names and other, key aspects of the Internet, were increasingly challenged due to their partial independence of governments. Recent decisions by ICANN, such as a massive liberalization of top-level domain names and the creation of the .xxx extension for pornography, have accelerated and exacerbated the debate over increased government involvement in the governance of the Internet, either through a dedicated UN agency, or through the International Telecommunications Union (ITU), an existing UN body in charge of ensuring international interconnection and facilitating the deployment of telecom infrastructure, and thus so far completely alien to the Internet world. Prominent individuals such as FCC Commissioner McDowell have made it clear that, should the multi-stakeholder model be abandoned, this would mean the end of the (free) Web as we know it.[2]

Not surprisingly, as the International Telecommunications Regulations (ITR) Treaty had to be re-discussed at the end of last year in the World Conference on International Telecommunications (WCIT), held in Dubai, the debate reached unprecedented peaks. Every stakeholder was looking for a different outcome: the ITU wished to expand its remit over the Internet, European Telecom operators wanted to secure more revenues by changing interconnection rules, China, Russia and India wanted stronger government control over the Internet architecture and content and many in the US and Europe stood to protect the multi-stakeholder model that made ICANN at once a very effective and increasingly controversial regulator. The confusion became chaos when a number of Africa, Middle East and Asian countries sought the inclusion of the declaration of Internet access as a fundamental human right in the new ITRs. When all this was finally translated into a proposed new ITR treaty, as many as 55 countries (including the US, Canada, Australia, the UK and many other EU countries) decided not to sign. Since then, the question is unresolved, and unlikely to be successfully addressed during 2013.

## Where do we go from here?

It is highly unlikely that the many problems that affect cyberspace today can be solved in one go. There are at least three aspects that deserve separate, international agreement: cyber-security, Internet governance and freedom of expression. Attempting to mix and match these three issues inevitably means failure. Conversely, solutions exist in all three domains, which would also preserve the consistency of the overall picture.

First, cybersecurity needs a global public-private partnership which entails the following steps:

- Countries should establish generic commitments to take action to fight botnets and refrain from engaging in government-sponsored cyberattacks.

[2] See "The UN Threat to Internet Freedom", *Wall Street Journal*, 21 February 2012 (http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html).

- All governments should set up Computer Emergency Readiness Teams (CERT) that receive notification from private parties and secure network resilience either directly (when they own the networks) or indirectly by remunerating network operators for their investments in network upgrade and security – something that seldom happens in telecom regulation today.
- Private operators should agree on industry-wide codes of conduct at regional and possibly global level to ensure that the flow of information between operators and public authorities is as fast and reliable as possible.
- Trust must be established between public and private operators through a dedicated platform, such as the European Public Private Partnership for Resilience (E3PR).
- A taxonomy and classification of major risks and available counter-strategies should be developed: this, in turn, would enable the development of a more mature insurance market for cybersecurity.

Second, there is no credible alternative to the multi-stakeholder model for Internet governance. But the United Stated should realise that key Internet assets should not be controlled only by US companies as is currently the case: while more than half of Internet users are located in Asia, the US still keep exclusivity over the Internet Assigned Numbers Authority (IANA) and the root zone file of the Internet. At a minimum, non-US companies, including EU-based ones, should be allowed to compete to become the managers of these critical resources. More generally, ICANN should become more transparent, structured, accountable and truly multi-stakeholder if it wants to survive as a private regulator: all eyes are on ICANN's procedures, and they cannot rely anymore on 'rough consensus' among Internet gurus and engineers.

Third, the global community should agree on principles and rights on Internet usage, including the need to guarantee that, whatever managed services run over the IP protocol, end users have at least a part of the Internet in which neutrality and the end-to-end architecture are preserved. This will be heavily resisted since it could lead to easier anonymity for criminals: but any alternative would mean killing democracy. This, in turn, means that the Web will increasingly look like a two-track world: the basic, end-to-end Internet, which should be protected for freedom of expression purposes; and managed cloud services, which will include many of the new features of IT-enabled economies, from smart transport to home automation and will feature enhanced levels of security and privacy through trusted traffic filtering.