COUNCIL on FOREIGN RELATIONS

Cybersecurity and Internet Governance

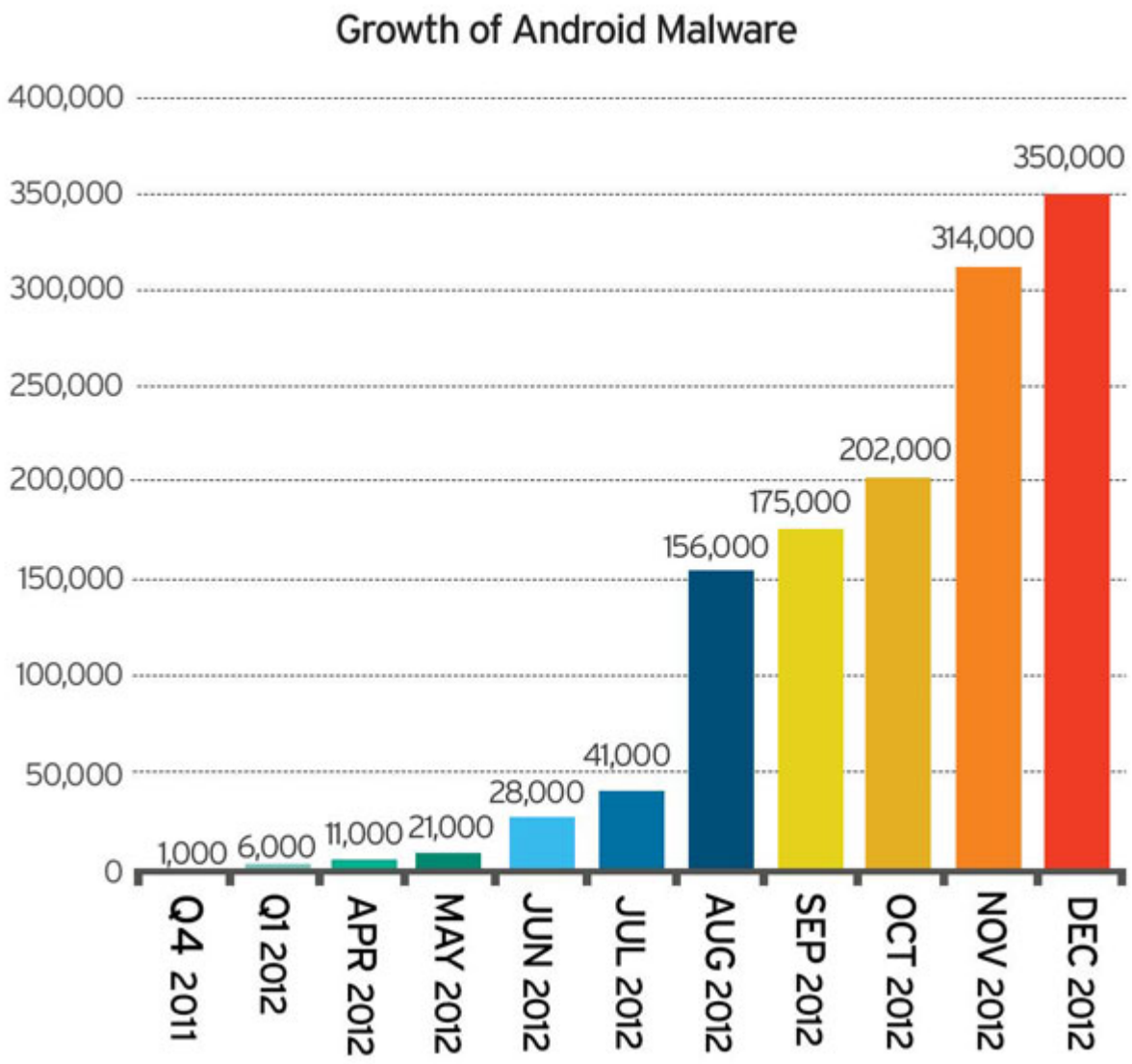
Author: Andrea Renda, Senior Research Fellow, Centre for European Policy Studies
May 3, 2013

Editor's note: This brief is a feature of ***the Council of Councils initiative****, gathering opinions from global experts on major international developments.*

Cybersecurity is now a leading concern for major economies. Reports indicate that hackers can target the U.S. Department of Justice or Iranian nuclear facilities just as easily as they can mine credit card data. Threats have risen as the Internet has become a critical infrastructure for the global economy, with thousands of operations migrating onto it. For example, the innocuous practice of bring-your-own-device to work presents mounting dangers due to malware attacks--software intended to corrupt computers.

Between April and December 2012, the types of threats detected on the Google Android platform increased by more than thirty 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. There is no doubt that the Internet is efficient. But it now needs a more concerted global effort to preserve its best aspects and guard against abuses.



Source: Trend Micro (2013)

The rise of the digital cold war

Cyber threats and cyberattacks also reveal an escalating **digital cold war**. For years the United States government has claimed that cyberattacks are mainly state-sponsored, initiated predominantly by China, Iran, and Russia. The penetration of the U.S. Internet technology market by corporations such as Huawei, subsidized by the Chinese government, has led to more fears that sensitive information is vulnerable. After an explicit exchange of views between President Barack Obama and President Xi Jinping in February 2013, the United States passed a new spending **law** that included a cyber espionage review process limiting U.S. government procurement of Chinese hardware.

U.S. suspicions intensified when Mandiant, a private information security firm, released a report detailing cyber espionage by a covert Chinese military unit against 100 U.S. companies and organizations. In March 2013, the U.S. government **announced** the creation of thirteen new teams of computer experts capable to retaliate if the United States were hit by a major attack.

On the other hand, Chinese experts **claim** to be the primary target of state-sponsored attacks, largely originating from the United States. But in reality the situation is more complex. Table 1 shows that cyberattacks in March 2013 were most frequently launched from Russia and Germany, followed by Taiwan and the United States.

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

What is happening to the Internet?

Created as a decentralized network, the Internet has been a difficult place for policymakers seeking to enforce the laws of the real world. Distributed Denial of Service (DDoS) attacks—consisting of virus infected systems (Botnet) targeting a single website leading to a **Denial of Service** for the end user—became a harsh reality by 2000, when companies such as Amazon, eBay, and **Yahoo!** had been affected. These costs stem from the direct financial damage caused by loss of revenue during an attack, disaster recovery costs associated with restoring a company's services, a loss of customers following an attack, and compensation payments to customers in the event of a violation of their service level

agreements.

As the Internet permeates everyday life, the stakes are becoming even higher. In a few years, society could delegate every aspect of life to information technology imagine driverless cars, machine-to-machine communications, and other trends that will lead to the interconnection of buildings to trains, and dishwashers to smartphones. This could open up these societies to previously unimaginable disruptive cyber events. What is as concerning is that in cyberspace, attacks seem to have a structural lead over defense capabilities: it can be prohibitively difficult to foresee where, how, and when attackers will strike.

Confronted with this challenge, the global community faces a dilemma. The neutrality of the Internet has proven to be a formidable ally of democracy, but the cost of protecting users' freedom is skyrocketing. Critical services, such as e-commerce or e-health, might never develop if users are not able to operate in a more secure environment. Moreover, some governments simply do not like ideas to circulate freely.

Besides the "**giant cage**" built by China to insulate its Internet users, countries like Pakistan have created national firewalls to monitor and filter the flow of information on the network. And even the Obama administration, which has most recently championed Internet freedom initiatives abroad, is **said** to be cooperating with private telecoms operators on Internet surveillance, and Congress is discussing a **new law** imposing information sharing between companies and government on end-user behavior, which violates user privacy.

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 requires a brief explanation of how the Internet is governed, and what might change.

The end of the Web as we know it?

Since its early days, the Internet has been largely unregulated by public authorities, becoming a matter for private self-regulation by engineers and experts, who for years have taken major decisions through unstructured procedures. No doubt, this has worked in the past. But as cyberspace started to expand, the stakes began to rise.

Informal bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN)—a private, U.S.-based multi-stakeholder association that rules on domain names and other major aspects of the Internet have been increasingly put under the spotlight. Recent ICANN rulings have exacerbated the debate over the need for more government involvement in Internet governance, either through a

dedicated United Nations agency or through the International Telecommunications Union (ITU), an existing UN body that ensures international communication and facilitates deployment of telecom infrastructure. But **many experts fear** that if a multi-stakeholder model is abandoned, the World Wide Web would cease to exist as we know it.

Last year's World Conference on International Telecommunications, held in Dubai, hosted a heated debate on the future of cyberspace. Every stakeholder was looking for a different outcome. The ITU looked to expand its authority over the Internet; European telecoms operators wanted to secure more revenues by changing the rules for exchanging information between networks; China, Russia, and India wanted stronger government control over the Internet; the United States and Europe stood to protect the multi-stakeholder model of ICANN; and a group of smaller countries sought to have Internet access declared a human right.

When a new treaty was finally put to vote, unsurprisingly, as many as fifty-five countries (including the United States and many EU member states) decided not to sign. Since then, the question on how the Internet will be governed remains unresolved.

Where do we go from here?

The problems that affect cyberspace cannot be resolved easily. There are three aspects that deserve international cooperation: cybersecurity, Internet governance, and freedom of expression. Solutions exist in all three domains, but should be addressed separately.

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

- Countries should formally commit to fighting botnets and refraining from government-sponsored cyberattacks.
- Governments should set up Computer Emergency Readiness Teams that receive notification from private parties and secure network resilience either directly or through private network operators.
- Operators should agree on industry-wide codes of conduct at a regional, and possibly at a global, level to ensure that the flow of information between operators and public authorities is fast and reliable.
- Trust should be established between public and private operators through a dedicated platform, as is **currently being adopted in Europe**.
- A taxonomy and classification of major risks and available counterstrategies should be

developed. This 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 States should realize that major Internet assets should not be controlled solely by domestic companies, especially as most Internet users are in Asia. More generally, ICANN should become more transparent, structured, accountable, and represent a multi-stakeholder framework if it wants to survive as a private regulator.

Third, the global community should protect freedom of expression, possibly through the United Nations Educational Scientific and Cultural Organization. Even if traffic management and "toll lanes" are allowed on the Internet, universal access to a robust, neutral Internet should always be preserved as a guarantee for democracy. This will be heavily resisted since it could lead to easier anonymity for criminals, but any alternative would undermine Internet freedom.