DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

TRUMP'S CYBERSECURITY POLICY: MULTIPLE RISKS FOR THE PROTECTION OF HUMAN RIGHTS

Posted on 9 Febbraio 2017 by Fabrizio Di Geronimo

The election of Donald Trump as the 45th President of the United States will bring many consequences from the point of view of foreign relations, of economic policies, of climate change and of military strategies. However, a fundamental policy that is not broadcasted by media as commonly as the other, is that concerning cybersecurity.

It is undeniable that cyber threats are becoming, day after day, an always more urgent issue. Technology is developing at an extraordinary pace and always more devices, private and public, are connected to the Internet, that meaning that they are possible target of a cyber attack. A fast consideration of the Internet of things, as well as of the interconnection of air traffic control system, nuclear power stations, train stations and electrical power grid should be enough to understand the importance of the problem since all these facilities could be attacked by a terrorist organizations or by an enemy State.

Cyber threats are constantly rising, as regard both the number and the intensity, and they are not exptected to reduce their pace during the next four years. The new US President Donald Trump would have, therefore, to approach the problem. It must be acknowledged, at least, that Donald

Trump considers cybersecurity as a high priority for his new presidency. It could not be different, considering the importance he attributes to security. What is at stake here is the ability of the 45th President to understand the importance and complexity of cyber threats and his capacity to fight them properly, without affecting excessively human rights. However, some recent events do certainly show that this is not the case, leaving no reasons to be optimistic.

What President Trump has done so far, was to acknowledge his lacking knowledge of the problem and to nominate a group of expert that shall provide a plan to enhance cybersecurity defenses of the United States. The head of this group is Rudy Giuliani, former Mayor of New York and expert of cybersecurity (the fact that his servers were hacked during the days of the appointment, it must be admitted, was also a political misfortune). His intention to fight cyber threats has been clearly stated in his first declarations, as also the will to secure an alliance with the private sector and to start a program of cyber education. Both these points are incredibly important. Indeed, the American private industry can (and must) play a fundamental role in the protection of cyberspace, because of their technical knowldege and of the criticality of some of the private businesses. Today is a matter of fact that the most important national critical infrastructures are owned or managed by the private sector that, therefore, cannot be left out in a discussion on cybersecurity.
In addition, the majority of cyber attacks are successful because of the inexperience and weak defenses of private users. A clear example of this trend is the history of Stuxnet, one of the most successful malware in the short history of cyber attacks. Designed, allegedly, by the United States and Israel, this malware was designed to sabotage the Programmable Logic Controller (PLC) S7-400 used by Iranian nuclear power plants to automate some functions. In order to attack this PLC, Stuxnet had to attack some facilities' computers. The strategy adopted was to infect personal computers of some employees of the targeted Iranian nuclear power plant and consequently their USB flash drives. In this manner, when the employees inserted their infected pen drive into the implant's computers, Stuxnet was able to attack them and, consequently the PLC,

reaching its aim to destroy and make unusable the Iranian nuclear power plants. Luckily the aim of Stuxnet was only to hinder the nuclear strategy of Iran during the negotiations of the notorious nuclear deal reached by President Obama. However, consequences could have been much worse, and only because of the infection of a private device. Therefore, the strategy to start a cooperation with both users and important companies seems to be reasonable and appropriate.

In addition, Trump has based his campaign also on cybersecurity, defining it “the future of warfare”. The website for his campaing specifies the intention to “order an immediate review of all U.S. cyber defenses and vulnerabilities, including critical infrastructure”, to “create Joint Task Forces” and to “evelop the offensive cyber capabilities we need to deter attacks by both state and non-state actors and, if necessary, to respond appropriately”.

To sum up, the proposed cybersecurity policy seems quite interesting and with smart proposals. However, some controversial points and elements cannot let us be optimistic on the future of cybersecurity.

One of the most controversial issue about Trump’s cybersecurity policy is strictly linked with his foreign relations one, and namely the ambiguous connection with Russia. During the entire electoral campaign, US democracy has been endangered by Russian hackers that tried to boycott the elections, succeding, at least partially, in their efforts. Even if it will remain uncertain whether Russian hackers were actually able to modify the electoral results thanks to a malware aimed at reprogramming the electronic counting machines, they did certainly manage to leak some private e-mails hacking the Democratic National Committee. In addition, it is worth noticing, this episode showed the potential of cyber threats to endanger the very functioning of US democracy, a threat that no one should take easily.

On the contrary, Trump has always denied the implication of Russia, even strongly criticizing the operation of US intelligence, and did never sided strongly against these kind of episodes. Trump’s statements look so unreasonable that also General Mattis, appointed to the Defense

Department, contradicted his President, defining Russia as a “key strategic competitor” with regard to cybesecurity. This entire incident shows either the will of Trump not to endanger a possible future relation with Russia (even at the expense of cybersecurity), or its inability to understand the seriousness of the problem. Moreover, after these stance, it is reasonable to consider that the declared will to “respond appropriately” to cyber attacks, developing “offensive cyber capabilities” will remain unexpressed whether contrasting with Trump’s idea of international relationship.
On the other side, Hillary Clinton clearly stated that America had “to invest in protecting our governmental networks and our national infrastructure …I want us to lead the world in setting the rules in cyberspace. If America doesn't, others will." The United States shall, indeed, use their negotiating power and international influence to promote the adoption of some international rules for the cyberspace and the regulation of cyber threats, as it has been recently done with the decision to consider a cyber attack as “an armed attack against one or more of them in Europe or North America”. That means that now, NATO intervention can be triggered also by a severe cyber attack.
Another fundamental problem that need to find a solution, as fast as possible, is that of accountability and punishment, again exemplified by the alleged Russian attacks. In cyberspace, because of the distance of the target and the possibility to use proxies, it is incredibly hard to attribute with certainty an attack, and therefore to punish the guilty. However, the United States, as the main target of cyber attacks (both from other States and private organizations) must necessarily do something in this regard, punishing more effectively cyber attackers, both on an international (i.e. diplomatic) and internal (i.e. criminal) point of view. A first attempt could be to update the Computer Fraud and Abuse Act, dating back to 1986. That will certainly reduce the threats.
Trump’s declaration on Russian hackers cannot be seen as a good step in that direction and in the enforcement of his (albeit good) electoral proposal.

The second episode relevant to understand Trump’s approach toward cybersecurity start with the request of the FBI to unlock the iPhone of the

shooter of San Bernardino. The 19 February, Trump wrote on his Twitter account, following similar public statements, "I use both iPhone & Samsung. If Apple doesn't give info to authorities on the terrorists I'll only be using Samsung until they give info" and invited to "oycott all Apple products until such time as Apple gives cellphone info to authorities regarding radical Islamic terrorist couple from Cal.". With these statements, he clearly showed his will to shift (even further) the balance between liberties and security toward security, totally disregarding some fundamental Supreme Court's decisions such as *United States v. Jones* (2012), but also *Rasul v. Bush* (2004), *Rumsfeld v. Padilla* (2004), *Hamdi v. Rumsfeld* (2004) and *Hamdan v. Rumsfeld* (2006). The new President committed the same mistake as regard mass surveillance, promoting the restoration of some amended part of the Patriot Act (one of the most controversial legislative act of all time), conerning the bulk collection of US citizens' phone data. He also argued in favor of the monitoring of mosques and of the creation of a huge database of all Muslims living in the US.

He showed to share that concept that has characterized legal responses to terrorism since 2001, ready to sacrifice rights and liberties acquired during years of suffering in the name of security, a very misinterpreted value. Trump demonstrated as well, as regard the specific case of fighting cyber threats, to reject encryption and data protection, to misunderstood the real issue of cybersecurity and to neglect the relationship between privacy and cybersecurity. Moreover, he potentially hinder possible fair relationship with the private sector, that must certainly be considered as the strenght of the United States as regard technology and as an essential partner in the fight to cyber threats. Again, Trump's actions seem to be in contrast with his proposed policy.

In conclusion, even if the proposed cybersecurity strategy did allow to be optimistics, some recents events and declarations do not. In particular, Trump decision to "err on the side of security" and his inexperience in the field of cyber threats will risk to endanger his same intention to ensure cybersecurity. It seems unlikely, indeed, that Trump's administration will realize the importance of encryption and data protection in order to reach

cybersecurity, that is far to be just a matter of surveillance and control. Moreover, the freedom on the Internet and the protection of fundamental rights would be at stake. In addition, his ambiguous relation with Russia and his outdated protectionism will constitute an hindrance to the role that the United States shall play, together with other actors such as the European Union, in the promotion of the web as a safe area of freedom, security and justice.
In other words, even if his declared aim was to enhance cybersecurity through a fundamental partnership with private industries, Trump acted against them with regard to encryption and freedom on the Internet; even if he stated the will to strenghten US capability of reprisal, his weak attitudine toward Russia discloses something else. To conclude, this inconsistency between Trump's proposed policy during the electoral campaign and his behavior reveals either the effect of populism in the field of cybersecurity or the inability of the new presidency to actually deal with the problem.

Article 5 NATO

18 U.S. Code § 1030