Aspenia
online
Pubblicata su *Aspenia online* (https://www.aspeninstitute.it/aspenia-online)

International cyber governance between sovereignty and new arrangements

Raffaele Marchetti - Global Issues - 29/12/2017

Cybersecurity is increasingly of central concern for governments, businesses and individuals. It is enough to know that 74% of businesses expect to be hacked each year. The estimated economic loss due to cybercrime is expected to reach approximately $3 trillion by 2020, with $400 billion lost annually[1]. And every year companies pay around $35,000 for protection against cyber threats. There is also a price to pay in terms of privacy: In 2015, the world witnessed a loss of 700 million personal data records[2]. Finally, a political link is becoming increasingly evident. From the American-Israeli case of the Stuxnet attack to the Iranian nuclear facilities to the current "Russiagate" in the USA, the political-strategic relevance of cybersecurity is generating hard controversies. In part, this is because of the current strategic context of "power transition" – away from the US-dominated "unipolar moment", with the center of gravity shifting toward Asia – which many view as extremely unstable. The historical record of the power transition from the declining hegemon to the revisionist power indicate that we have 75% of possibilities to end up in a major world conflict[3]. Predictions about the future world order are bleak.

In this context, in the cyber world, we are seeing the multiplication of offensive power in the hands of a few technologically-advanced countries that are in a state of growing rivalry. A typical phenomenon of our time is cyber foreign policy by proxy. All powerful countries have done it, and all have pointed fingers at others for doing the same. According to Cyber Operation Tracker, since 2005, 16 countries in more than 150 instances have directly or indirectly used cyber techniques to interfere in the domestic affairs of other countries. The countries are China, France, India, Iran, Israel, Kazakhstan, North Korea, South Korea, Mexico, Russia, Spain, Taiwan, the United Arab Emirates, the United Kingdom, the USA and Vietnam. Military and civilian espionage, political destabilization, and sabotage of critical infrastructures are becoming common practices.

In response, elements of cyber global governance have been fostered in recent decades, but without any universal agreement.

At the multilateral level, several steps have been taken. In 1998, Russia proposed an "information weapons" control treaty at the UN, though it was rejected by Western countries. In 2015, a UN Group of Governmental Experts (GGE) proposed a set of recommendations "aimed at promoting an open, secure, stable, accessible and peaceful ICT environment". The EU worked on the issue through a 2016 directive on the security of network and information systems. The Shanghai Cooperation Organization has issued two different codes of conduct. The Council of Europe approved the Budapest Convention on Cybercrime. NATO produced the Tallin Manual to apply international law to cybercrime. The G20 has repeatedly addressed the issue since 2015. And, finally, OSCE issued the Istanbul final declaration and resolution on cyber security in 2013.

At the bilateral level, there have been other significant initiatives. In 2015, the US and China agreed on a set of regulations against cyberespionage related to the theft of intellectual property (which subsequently endorsed by the G20). Also in 2015, Russia and China agreed on an international information security protocol and Australia and the Netherlands did the same at The Hague conference on cybersecurity.

In addition, there are multi-stakeholder fora that are producing norms. Intense discussions are underway at the Internet Corporation for Assigned Names and Numbers, the Internet Assigned Numbers Authority and the International Telecommunications Union. Relevant is also the "voluntary framework" for critical infrastructure cybersecurity by the National Institute of Standards and Technology.

In sum, what is emerging is an uneven set of arrangements at various levels: national regulations, international laws, professional standards, purely political agreements, and technical protocols. Clear positions and harsh debates are however characterizing such arrangements ("regime complex"). The US, for instance, is particularly active on the promotion of norms against cyberespionage for commercial advantage. Worth noting is the ongoing shift in norms on encryption: originally a pro-encryption position was dominant and tied to economic and national security, but today, especially after 2015 terrorist attacks, "encryption as a threat" is gaining more attention. Just as intense is the debate on the legitimacy of aggressive cybersecurity. Aggressive war is considered illegitimate in international law, therefore preemptive and preventive war are also deemed illegitimate. But was Stuxnet legitimate? A number of NATO members are currently considering proposals to make cyberattacks legitimate under specific circumstances. The debate is open.

Two alternative visions proposed by the tech company world can be detected in the debate, captured, on one extreme, by Dan Smith, President of Microsoft (who proposes a Digital Geneva Convention) and on the other by Nathalia Kaspersky, founder of Kaspersky Lab (who calls for "cyber sovereignty").

Smith has called on the world's governments to implement international rules to protect civilian use of the internet. As much as the 4th Geneva Convention protected civilians in times of war, the Digital Geneva Convention would protect civilians in times of peace. For wars, crucial assistance was provided by the Red Cross; for cyber, it would be the active assistance of technology companies. Smith's proposal is focused on six points: 1) No targeting of tech companies, private sector, or critical infrastructures; 2) Assist private sector efforts to detect, contain, respond to, and recover from events; 3) Report vulnerabilities to vendors rather than to stockpile, sell or exploit them; 4) Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable; 5) Commit to nonproliferation activities to cyber weapons; and 6) Limit offensive operation to avoid a mass event. Ultimately, this would entail the creation of a new institution, something like the International Atomic Energy Agency, to address the issue of public attribution.

Kaspersky's proposal is starkly different and is centered on the value of cyber sovereignty. From her perspective, the world is divided in two clubs, the one composed of a handful of cyber sovereign nations, the other of countries bound to remain cyber colonies due to their technological backwardness. In such a situation, any attempt to generate global regulations would consolidate political hegemony. Underpinning this position is a significant mistrust in global regulatory frameworks as they are seen as tools of domination. In such context, the tradition principle of self-reliance remains the best normative reference. It continues to be the best way to guarantee national sovereignty. The support of the so-called "national champions", or national tech companies that guarantee cyber sovereignty, remains a crucial, unavoidable step in a rivalrous and competitive world.

Different observations can be formulated on the tension between global regulation vs cyber sovereignty. First, cybersecurity is clearly controversial because now it has become a global game. Second, it has no one domain. It follows the patterns of global politics. Third, cyber development will likely create an even more inequality between countries with high levels of digital technology and those without. Fourth, cyber regulation remains a state activity as long as infrastructures are territorial and physical (the Chinese Great Firewall, for example). Fifth, states remain insufficiently incentivized to reach agreements because they can profit from the vacuum. Sixth, a process that might lead to global regulation leads one to see cyber sovereignty is a sine qua non element for global rules. As the weapons conventions on non-proliferation in the 1960s were possible only because the two cold war rivals were seeking strategic parity, the contenders here must recognize a mutual reciprocal vulnerability to allow global regulations to emerge. Only on the bases of strong cyber sovereignty it will be possible to negotiate

We are in a transition period characterized by a decreasing trust among the major world powers. At least as from 2008, the world has drifted apart: This has been a very difficult decade of polarization. However, to build collective institutional responses to the cyber crises based on the triple principle of confidentiality, integrity and availability, a certain degree of trust is needed. Such trust will come only after there is reciprocal recognition among countries that they are fully cyber sovereign, hence reciprocally vulnerable.

---

[1] Center For Strategic & International Studies, Net Losses: Estimating The Global Cost Of Cybercrime 6 (June 2014), at http://www.mcafee.com/us/resources/reports/rp-economicimpact-cybercrime2....

[2] Gemalto Releases Findings of 2015 Breach Level Index (Feb. 23, 2016), at http://www.gemalto.com/ press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx.

[3] G. Allison (2017) Destined for War: Can America and China Escape Thucydides's Trap?, Houghton Mifflin Harcourt.

Read also:

Knowing the nation: data and the need for vision
Victor Broers

Thus Donald Trump joined the global conflict on technology
Eric B. Schnurer

URL di origine: https://www.aspeninstitute.it/aspenia-online/article/international-cyber-governance-between-sovereignty-and-new-arrangements

Links:
[1] https://www.aspeninstitute.it/aspenia-online/contributors/raffaele-marchetti
[2] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftn1
[3] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftn2
[4] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftn3
[5] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftnref1
[6] http://www.mcafee.com/us/resources/reports/rp-economicimpact-cybercrime2.pdf
[7] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftnref2
[8] http://www.gemalto.com/
[9] https://www.aspeninstitute.it/X:/Articles and workplan/2017/12 Dic/Cybersecurity/Marchetti_eng.docx#_ftnref3
[10] https://www.aspeninstitute.it/aspenia-online/article/knowing-nation-data-and-need-vision
[11] https://www.aspeninstitute.it/aspenia-online/contributors/victor-broers
[12] https://www.aspeninstitute.it/aspenia-online/article/thus-donald-trump-joined-global-conflict-technology
[13] https://www.aspeninstitute.it/aspenia-online/contributors/eric-b-schnurer
[14] https://www.aspeninstitute.it/aspenia-online/image/cg

[15] https://www.aspeninstitute.it/aspenia-online/article/spying-through-microwave-intelligence-gathering-online-world
[16] https://www.aspeninstitute.it/aspenia-online/article/cyberwar-nuova-guerra-fredda-o-scontro-politico-interno
[17] https://www.aspeninstitute.it/aspenia-online/article/cyber-intelligence-e-potere-culturale-comprendere-il-mondo

Links - other articles by this author:
https://www.aspeninstitute.it/aspenia-online/article/international-cyber-governance-between-sovereignty-and-new-arrangements
https://www.aspeninstitute.it/aspenia-online/article/la-nuova-duma-la-continuit%C3%A0-di-putin-e-il-fattore-astensione