Posted on the CEEEP website
Date: October 15, 2021

THINK TANK DEL EJÉRCITO DEL PERÚ

Future World: The Threat of Cyberattacks in a Hyperconnected Society

Mariano López de Miguel, is a historian with a master's degree in Contemporary History from the University of Cantabria, a specialist in conflicts in Eastern Europe (Ukraine, the Balkans and the former Yugoslavia), the Caucasus (Chechnya, Abkhazia and Georgia) and the Middle East (mainly in the concerning the Arab-Israeli conflict). He is also a doctoral researcher at the University of Murcia and a member of the Editorial Board of the Online Blog "Conversation on History". He is currently studying for a doctorate at the Faculty of Philosophy and Letters of the University of Murcia.

Translated by Claudia Iwasaki

Summary

Since the introduction of the *World Wide Web* in homes at the end of 1995, the Internet has evolved geometrically, leading the world to a state of hyperconnectivity called by renowned futurologists, such as Herman Kahn or Marshall McLuhan, as "The Global Village". However, these societies are not without risk: From the arrival of information highways to the dangers based on cyberattacks, they have transformed the social, political and defense culture on how to act in the face of these attacks. Since 2016, cyberattacks have multiplied by hundreds, thus demonstrating the fragility of the planet in the face of an enemy that does not necessarily have a physical presence, and that acquires an advantage due to the opportunity offered by anonymity. Undoubtedly, the world is facing a new battlefield within the so-called irregular wars or asymmetric conflicts.

Keywords

World Wide Web, Social networks, Hyperconnectivity, Cyberattacks, National Security.

Introduction

On October 4th, 2021, billions of users – worldwide - were prevented from accessing their main social networks, such as Facebook, Instagram and WhatsApp (all of them run by billionaire entrepreneur Mark Zuckerberg) for - at least - six hours. These applications collapsed when a failure, unidentified to date (October 5th, 2021), made it impossible to establish connection with them through *apps* and web browsers. This fact, far from being isolated – since it is the fourth massive fall of these applications and direct messaging programs since 2016 – demonstrates an increasingly present reality: The absolute dependence on new communication technologies by an increasingly broad sector of society, in what Marshall MacLuhan called - four decades ago - "The Global Village"

Analysis

More than a quarter of a century ago, new technologies made their way through the "democratization" of the *World Wide Web* or, as it is commonly known, the internet. In 1990, the British computer scientist Tim Berners-Lee established the first communication between a client and a server utilizing the HTTP protocol (Hypertext Transfer Protocol), to which the possibility of uploading/loading graphics and images was added, to be an almost exclusive project of the defense departments of Western countries (mainly the US DARPA) to be a valuable tool for global use, allowing the opening of the internet to civil society and, mainly, to world trade.

Later, the text forums would appear, the first search engines such as Yahoo! or the extinct AltaVista, in addition to other possibilities, which were suddenly slowed down after the terrible explosion of the bubble of the dot-com companies in mid-2000[1]. This situation showed that, although new technologies had a wide range of possibilities, they also accumulated a risk index of 6/6 (with 1 being the minimum risk and 6 the maximum). Additionally, the implementation of the internet worldwide was not without controversy. Developing countries, mainly in the MENA region (North Africa and the Middle East), complained bitterly about the scarcity of investment to provide access to the *World Wide Web* compared to neighboring countries such as Israel where, as of October 2000, about 67% of the population had access to the network.

However, one of the factors in the rise of the Internet at that time was the creation of the first international Arabic-language news channel (the Qatari network Al Jazeera). Their reports were among the first to be seen both through satellite television and through direct download videos in an era before the audiovisual giant of YouTube. The other fact that caused a geopolitical earthquake was the terrible attack of September 11th, 2000, which increased the development of the Internet within a civil-military synergy.

Although the creation of draconian laws for the sake of national security, such as the infamous American "Patriot Act", aroused suspicion among users who sought to protect their security, it would not be until the period of 2004-2009 when the remarkable takeoff of the Internet took place at an almost universal level. The post-war and US military occupation of the Republic of Iraq would lead to the insurgency in the country turning to the web to upload its contents, which included from attacks on coalition troops to the infamous hostage executions carried out by the *Ansar Al Sunna* group of Abu Musab Al Zarqawi.

The anonymity when uploading such content gave rise to the Internet becoming a propaganda tool for fundamentalists, from Iraq to Afghanistan, or other focus of "Global *Jihad*" such as Chechnya, Mindanao in the Philippines or Uzbekistan in Central Asia. The appearance of video portals such as YouTube,

Google Video or Vimeo, together with alternative mail servers and the beginning of the first social networks such as Facebook or Twitter, would allow uploading content of all kinds. And although those that showed high rates of violence were quickly eliminated, their dissemination had been massive in a few minutes. During that same time, former U.S. counterterrorism czar Richard A. Clarke warned of the need to invest at least 1.1% of each country's GDP in cyber defense funds.

In April 2007,the first wake-up call would be given in Estonia, through an attack allegedly carried out from Russia. This aggression showed *"how easy it is for a hostile country to take advantage of potential tensions within a society to cause harm*."[2] The websites for banks, media outlets and government agencies collapsed due to unprecedented levels of internet traffic. Networks of computer bots — known as *botnets* — sent massive amounts of junk messages *(spam)* and automatic *online* orders to clutter up servers. The result was that Estonians were left unable to use ATMs and telematic financial services.

The 2007 bombings were conducted from Russian IP addresses, *online* instructions were in Russian, and the Russian federal government ignored Estonia's calls for help. However, there was never concrete evidence that these attacks were carried out by the Russian government. It would not be the last time that the Moscow government was accused of cyberattacks. Later, in 2009 during the conflict between Russia and Georgia over the rebel region of South Ossetia, Moscow – allegedly - carried out another aggression: collapsing several social networks in retaliation against a Georgian blogger, known as "*CYXYMU*" (Cyrillic name of Sukhumi, capital of another rebel region, the Republic of Abkhazia)[3]. The attacks were in response to texts in which *CYXYMU* accused Russia of militarily invading Georgia to wrestle these regions away, de facto independent since 1991, after the Soviet implosion.

Also, during 2009, the power of new technologies and social networks or *microblogging* channels was demonstrated after the demonstrations of the "green movement" in Iran, in protest against the fraudulent re-election of Mahmoud Ahmadinejad, along with the "new muscle" of dissidents in Egypt, after almost 30 years of autocratic governments of Hosni Mubarak. In fact, it would be in Egypt where digital activists would suffer their "first martyr" in the figure of computer programming student Khaled Said, who was brutally tortured in the police station in the Cairo neighborhood of Sidi Gaber.

There is no doubt that blogs, social networks and direct messaging applications had a major importance in the events that would give rise to the failed "Arab Spring". Countries such as Egypt, Tunisia, Libya, Syria, Iraq and Iran, through mandates that denied all democratic guarantees and freedom of expression, blocked hundreds of civic opposition websites and completely shut down internet access ("lockdown"), among which the provisions given by Hosni Mubarak, in January 2011, stand out, as well as by Bashar Al Assad, between April 2011 and 2012.

After the "Web 2.0" would come the normalization and massification of the use of *apps* of all kinds, following the second Iraqi civil war (2014 - 2017) and the global attacks conducted by the so-called "Islamic State", a terrorist group of jihadist affiliation with an apocalyptic vision of society, and that controlled much of the Syrian-Iraqi territory along with various provinces of nation-states such as Libya, Nigeria, Afghanistan or Tunisia. In that sense, the leader of the group, Abu Bakr Al Baghdadi, demonstrated his technological skills inherited from his "ideological father", Abu Musab Al Zarqawi. In the wake of these events, Western governments were faced with a very worrying legal situation: the law to hinder certain access to extremist web content (on the possible curtailment of freedoms and rights of citizens) or to review one by one the contents classified as harmful to national security, which would require a millionaire investment in tracking and tracking devices.

As if that were not enough, the specter of a possible Russian interference through cyberspace during the 2016 US presidential election, which would give victory to populist tycoon Donald J. Trump, and the problems during the referendum of leaving the European Union by the United Kingdom – known colloquially as "*Brexit*" – made more than a few security analysts and chiefs of staff of the respective nations speak of the basic need to direct more funds to cybersecurity, in addition to urgently creating departments dedicated solely and exclusively to network surveillance.

Conclusions

The latest cyberattacks suffered by the West since 2013 (whether they are acts of retaliation such as the North Korean hackers who stormed the digital headquarters of *Sony Pictures* for offenses of a film towards Supreme Leader Kim Jong Un, or those carried out by the intelligence branch of the Iranian *Quds* Force after the collapse of the Natanz Nuclear Complex, through the Stuxnet virus), together with the fall of the main social networks and direct messaging services for several hours on October 4th, 2021 make it clear how necessary it is to create a cybersecurity culture. While it is true that the CEOs of these companies attributed the fall to widespread human failure in their servers, the fact that a White House spokeswoman spoke during the first hours of a possible attack on the network or DNS collapse - also mentioned by CNN - did nothing but raise doubts and suspicions, as well as costing the founders of these technological oligopolies a whopping $7 billion in losses from the New York Technology Exchange (NASDAQ).

Another aspect to highlight is the total dependence of society on services such as WhatsApp, being curiously the direct messaging tool a labor alternative to the supposedly obsolete email. All of this without knowing the numerous security breaches in this application. Historical experience teaches that absolute dependence on a technology or energy source can transform developed nations into giants with feet of clay, such as the cases of shortage

of respirators during the COVID-19 pandemic or the double crisis of 1973 and 1979 due to the lack of oil.

Therefore, the reasonable use of new technologies by the world's population, as well as the fact that the developers of these technologies base their principles on sustainable models and that countries invest in cyber defense should be the logical response to this new challenge after the financial collapse of 2008 - 2013 and the health emergency of 2020.

Final Notes

[1] Matthew Lynn, "Las lecciones de la 'burbuja puntocom' veinte años después ," *El Economista* (january 22, 2020), https://www.eleconomista.es/opinion-blogs/noticias/10313700/01/20/Las-lecciones-de-la-burbuja-puntocom-veinte-anos-despues.html

[2] Damien McGuinness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país," *BBC News* (may 06, 2017), https://www.bbc.com/mundo/noticias-39800133

[3] Reuters Staff, "Bloguero georgiano víctima de ciberataque dice no le silenciarán," *Reuters* (august 12, 2009), https://www.reuters.com/article/internet-georgia-bloguero-idLTASIE57B2E520090812

Recommended bibliography

- Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (2010)
- Robert H. Latiff, *Future War: Preparing for the New Global Battlefield* (2017)
- Frederick Hodges and John R.Allen, *Future War and the Defence of Europe* (2020)