Economic and social impact of internet blackout: the case of the 2007 cyberattacks on Estonia and the 2008 SEA-ME-WE3 submarine cable disruption

Introduction

If we look back at the past and the strengths of the great empires or states that have succeeded one another over the centuries, there is a constant in the ability of the few to rise above their weaker enemies and allies. Ancient Rome, the British empire and, today, the world's greatest powers are united by **communication routes**. The information society in which we live and work presupposes the existence and permanent functioning of a digital infrastructure capable of connecting all the nodes of the network, keeping the entire architecture in constant operation.

Nowadays, those who control the net, or rather the digital roads, have the power to change the political balance of nations, to destabilise economies and to prevent the masses in revolt from asserting their rights against despotic, Orwellian governments. The gold of the 21st century is represented by data, by the information passing through digital infrastructures, largely embodied by submarine communication cables, "the great submarine electronic highways connecting the continents"[1], the "central nervous system of global telecommunications"[2].

Two emblematic cases will be presented below that aim to outline the economic and social impact of the interruption of network services on the populations affected: the cyber attack on Estonia in 2007, and the incident on the SEA-ME-WE3 submarine cable in 2008.

To measure this impact, we used a tool developed in collaboration between *The Internet Society*[3] and *Netblocks*[4], the ***Cost of Shutdown Tool***[5]: this is an online tool that estimates the economic impact of Internet shutdown as a whole, or of specific apps, basing the calculation on indicators obtained from the World Bank, the ITU (International Telecommunications Union), Eurostat and the U.S. Census[6].

It was created on the basis of research carried out by CIPESA[7] (Collaboration on International ICT Policy in East and Southern Africa) and by The Brookings Institution[8]. The Cost of Shutdown Tool is based on several costing equations, but the one examined here is for the case of a national shutdown (***National Internet Shutdown Costs***).

It consists of:

$$National\,GDP \times Duration \times Extent\,of\,Digital\,Economy \times Multiplier$$

Where:

- GDP: gross domestic product of the country under study;
- Duration: measured as the percentage of the number of days the shutdown occurred over the whole year;
- Extent of the digital economy in the country: calculated as the percentage of the national economy that is digital-based;
- Multiplier: according to the calculations of Professor John Quelch of Harvard Business School who estimated that the effect of each digital-related job contributes about 1.54 more jobs in other economic sectors.

To provide a significant example of the magnitude that a national shutdown could cause in economic terms for the affected country, it could be considered as a benchmark the United States of America GDP which amounts to 21.374 trillion \$ in 2019[9]. With around 6% of the entire GDP of the US coming from the digital economy, if an eventuality such as the one described above were to occur and last for seven days, the US would lose around 51 billion \$. If the disruption lasted for a whole year, this disastrous impact is estimated to be equivalent to $2\,659\,615\,244\,640$ (2.7 trillion \$)[10]. As a comparison, it would be equivalent to the construction of about 255 new multi-specialist hospitals of 450 beds each of medium-high complexity built, for example, in Italy[11].

Case Study: Cyber attack Estonia

In spring 2007, Estonia was the target of a cyberattacks campaign amounting to a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia, but the trigger for the attacks was the Estonian government's decision to move a monument to Soviet troops from the centre of Tallinn to a nearby military cemetery. The monument, representing a Soviet soldier, was originally erected in 1947 on the burial site of Soviet troops who fell during the capture of Tallinn during World War II. For the local Russian minority, the monument represents the 'liberator', instead for Estonians it is a symbol of oppression. On 27th April cyber attacks against Estonia's information systems begins and it is to be mentioned that these kind of attacks lasted for a total of 22 days. Although the types of attack were well known, they were unmatched in size and variety by a country as Estonia.

The Estonian context is characterised by strong digitalisation, for this reason a large-scale attack on the availability of public digital services has had a significant effect on the lifestyle of citizens and businesses[12]. In Estonia 97% of banking transactions take place online, in 2007, 60% of the country's population used the Internet at least once a day. As a matter of fact Mihkel Tammet, the IT director of the Estonian Ministry of Defence, explains that the Estonian state relies so heavily on the Internet that its model of government operations is referred to as "paperless government"[13]. In general, the techniques used in these attacks can be classified as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. Target systems included: web servers, e-mail servers, DNS servers and routers. In addition, the attacks have been targeted at various actors including the government, the president, the parliament, the police, banks, internet service providers (ISP), and online media. They have also caused damage to many small businesses and local government sites. To counteract this problem, some banks had to resort to temporarily blocking all foreign traffic, while remaining available to customers in Estonia. Then, the whitelist was gradually expanded to include also countries with a limited number of customers[12]. In the case of Estonia, the cyber-terrorist attacks occurred through the use of Botnets which were globally dispersed and virtually unidentifiable 'zombie' computers. The hackers hijacked computers (including many home PCs) in places like Egypt, Russia and the United States and used them in a DDoS strategy. Government and bank websites that normally received 1000 visits per day were "flooded" with more than 2000 requests per second.

The economic damage was difficult to be quantifed, but at the same time Estonia and the EU were widely credited for their ability to deal with this kind of emergency[14]. The bank loss which is known was to be estimated about 1 million $, and the attacks also blocked credit card and ATM transactions for several days[13]. In an attempt to assess the economic damage a steady GDP growth in previous years and a reversal in the year of the cyber attack emerged. It should be noted, however, that the downward trend in growth rates started a few quarters before the attacks and continued into the financial crisis which led Estonian GDP to a heavy -14.1% in 2009. According to an Estonian report that can be attributed to the Ministry of Finance, the economic return of Russia in the context of the recession in Estonia was measured in terms of GDP between 1% and 3.5%; however also in this case, these reductions are not exclusively attributable to cyber attacks[15].

Due to lack of an official estimate of the total cost caused by cyber attacks, we tried to find a lower bound using the Cost of Shutdown Tool and assuming some hypothetical conditions. We consider only the day when the attacks were most intense and continuous; besides, we consider an interruption of 50% of IT services, because the attacks did not block the whole bandwidth (during the all period of 22 days). Given the following variables, according to the Cost of Shutdown Tool, we find the following lower bound as a cost for the country: $31\,784\,249$ $. Such an estimate is underrated so it should be clear the overall extent of damage caused by the attacks.

Case Study: SEA-ME-WE3 submarine cable disruption

Submarine cables account for 99% of all international voice and data traffic of 7.7 billion people[2]. Ownership of these cables, which cover about $900\,000$ km of seabed, belongs to those who lay them, while they are managed by those who provide the information flows[2][17]. Their importance derives from the fact that their interruption or failure, however brief, interrupts a huge flow of terabytes per second of data of all kinds. Financial data, data relating to electronic transactions, the functioning of entire ministries in different countries around the globe suddenly stop being exchanged, leading to enormous losses and inconvenience.

A similar event occurred in 2008 when a whole series of submarine cables broke down between January and February: FLAG FEA, GO-1, SEA-ME-WE3, SEA-ME-WE4, FALCON, DOHA-HALOUL[16][20]. Italy was most closely affected by the SEA-ME-WE3 cable breakdown which connects Alexandria with Sicily (Mazara del Vallo). The interruption occurred on 19th December and also involved the SEA-ME-WE4 cable. The two aforementioned cables carry Internet traffic from Europe throughout the Middle East and their interruption caused the blockage of 70% of the network traffic in Egypt and it has stopped 60% of Indian services and caused disruption in some Gulf countries[18][19]. Two Egyptian stock exchange traders said financial transactions had slowed considerably.

The 'Cost of Shutdown Tool' was used to estimate the economic impact of the outage for 70% and 60% of the bandwidth in Egypt and in India respectively. This reduction lasted for a whole day. The cost of shutting down the Internet was calculated on a daily basis and then the percentage of bandwidth cut was taken into account. This resulted in a total cost for Egypt and India of $103,074,206$ \$ and $607,343,248$ \$ respectively.

Conclusions

To be able to quantify the damage caused in terms of both prevention and repair is highlithed by the recent Russian attacks and Google outage. The Cost of Shutdown Tool is proving to be a useful tool for estimating the costs of outages, the causes of which can be very diverse, as previous case studies have shown. A double damage for all authoritarian countries that shut down the internet in order to control society is underlined:

1. social damage: the emergence of ideologies and currents of thought aimed at improving and renewing an authoritarian and retrograde power is prevented, with the intention of isolating minorities.

2. economic damage: the Cost of Shutdown Tool shows that the longer the Internet is blocked, the higher the costs.

The recent Sars-Cov-2 pandemic has highlighted the need to accelerate the transformation processes towards a digitised society. With reference to the Italian context, one might only think of the difficulties encountered in the DAD and the consequent acceleration aimed at enhancing IT services. It is conceivable that similar pandemic events will have to be faced more and more, and the sudden cut in bandwidth will have an even greater impact on society. It is therefore clear that countries need to make an effort to prevent such events and to estimate their costs for insurance purposes.

Bibliografia

[1] Pierangelo Soldavini, Non solo bit: ecco come funziona la struttura globale di internet.

[2] Milena Gabanelli, I dati di quasi 8 miliardi di persone passano nei cavi sottomarini. Chi li controlla?

[3] The Internet Society https://www.internetsociety.org/

[4] NetBlocks https://netblocks.org/

[5] Cost of Shutdown Tool - NetBlocks https://netblocks.org/cost/

[6] COST: The Cost of Shutdown Tool - NetBlocks https://netblocks.org/projects/cost/

[7] The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) https://cipesa.org/

[8] The Brookings Institution https://www.brookings.edu/

[9] The World Bank USA GDP https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US

[10] Internet shutdowns cost countries $2.4 billion last year http://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

[11] Costi teorici di costruzione e di manutenzione nel 2017 http://www.byterfly.eu/islandora/object/librib:822955/datastream/PDF/content/librib_822955.pdf

[12] Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", Rain Ottis, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[13] Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses Multinational Responses. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

[14] "2007 cyber attacks on Estonia" https://www.stratcomcoe.org

[15] "The Estonian Cyberattacks", Andreas Schmidt, Delft University of Technology. https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

[16] Submarine cables map
https://www.submarinecablemap.com/

[17] Rebecca Mantovani, Tecnologia Telecomunicazioni: Internet viaggia lungo i cavi sottomarini.

[18] Gianni Rusconi, Quando Internet e la voce viaggiano sott'acqua.

[19] Marco Sommani, Istituto Informatica Telematica CNR Pisa, L'India rimane senza internet.

[20] Wikipedia, Rottura di cavi sottomarini internazionali del 2008 https://it.wikipedia.org/wiki/Rottura_di_cavi_sottomarini_internazionali_del_2008