CSS CYBER DEFENSE PROJECT

Trend Analysis

Cybersecurity at Big Events

Zürich, November 2019

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Alice Crelier

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css.info@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zurich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Alice Crelier (2019) Trend Analysis: Cybersecurity at Big Events, November 2019, Center for Security Studies (CSS), ETH Zurich.

Table of Contents

Executive Summary

Objective and Methods

As Big Events (BEs) like the Olympic Games or G20 Summits become increasingly digitalized, concern is growing among officials and academics about cybersecurity. This is unsurprising, because a growing number of unsecured and unsafe programs, applications and devices and an overall lack of cyber-hygiene open the door for the proliferation of nefarious cyber activities related to such BEs. Moreover, BEs are so important for both organizers and host countries (in terms of cost, mediated reach, reputational significance, soft power, etc.) that their associated cybersecurity aspects cannot be neglected, making BEs a particularly interesting object of exploration in the context of cybersecurity.

Consequently, this Trend Analysis (TA) aims to address the main issues regarding cybersecurity at BEs, using the G20 Leaders' Summits and the Olympic Games between 2009 and 2019 as case studies. This TA intends to answer the following questions: What is a BE and what are its various dimensions? Are there trends in cybersecurity organization and processes related to BEs? What trends can be observed in terms of the cyber threat landscape of BEs? What do they teach us about current and future cybersecurity at BEs?

This TA is based on an extensive literature review and analysis of a wide spectrum of white papers, journalistic coverage and academic literature.

It should be noted that this TA focuses on BEs themselves rather than on the general services on which they depend (e.g. transport, IT services, food supply, hotels, etc.).

Results

Overall, the paper points to the following key findings: First, the literature with regard to BEs is not extensive and mainly addresses sporting events, tourism and urbanism.

Second, there is no holistic definition of BEs that would include both the Olympic Games and the G20 Summits. Consequently, this paper defines the concept of BEs and its various dimensions as follows: BEs are "*ambulatory occasions of a fixed duration that a) attract a large number of visitors, b) have large* (and international) *mediated reach, c) come with large costs […], d) have large impacts on the built environment and population*", e) attract significant numbers of international attendees and spectators, f) exert political influence, and g) have cross-sectoral implications (Müller, 2015, p. 629).

Third, trends have shown that both G20 Summits and Olympic Games have expanded their cybersecurity organization and processes over the past decade.

Fourth, a comparative analysis and incident timelines indicate that, both the Olympics and the G20 Summits were affected by largely the same types of cyber incidents. The difference lies in the fact that G20-related attacks mostly involve cyberespionage and are less aimed at disrupting the Summits or damaging the image of the G20 or host countries, as is evidenced by trends regarding cyberattacks and cyber incidents. Olympic Games-related attacks mostly have a cybercrime background and are aimed at disrupting the Games or damaging the image of the Olympics or host countries. However, the number of cyberattacks of a political nature should not be underestimated, even in the context of sporting events.

Fifth, analyzing the cybersecurity-related organizational aspects and processes of the Olympic Games and G20 Summits as well as the associated threat landscape helps to highlight the following organizational prerogatives for cybersecurity at BEs:

- Plan early
- Prioritize cooperation and information sharing among the public and private sectors, industry and other non-state actors
- Create a shared mission and common cybersecurity goals
- Establish clear roles and responsibilities among stakeholders
- Incorporate cybersecurity into broader security planning (Dion-Schwarz, 2018, p. xii)
- Include all levels of government in the CERT
- Include subsidiarity in processes
- Identify the threat actors and their motivations/scopes
- Adopt a holistic risk assessment framework
- Consider geopolitical factors as central

Finally, BEs must be understood from a systemic perspective, especially given that these events depend directly and indirectly on their social context and have complex and unpredictable impacts on it.

1 Introduction

Big Events (BEs) are not intrinsically a new phenomenon. Indeed, there has been a strong tradition of Big Events in both European countries and the USA since the 19th century, with the Paris International Expositions, the Brussels International Expositions, the World's Fairs, the Olympic Games (starting in the 20th century), international political forums, etc.

Until World War II, events of these types, especially exhibitions and games, were organized to showcase the culture, technological innovations and industrial power of host countries. Events were attended by large numbers of visitors – ranging from 5 to 30 million – and vast numbers of countries participated. Host countries would spend significant resources on the organization of such events in order to "demonstrate their power". This was true in the past and is all the more so today. For example, Expo Milano 2015, an international registered exhibition hosted by Milan, attracted more than 22 million visitors and 145 participating countries with an official budget of €1.486 million (Expo 2015 S.p.A, 2018). Another, current example is the 2020 Tokyo Olympic Games with a budget reaching some €6.33 billion and around 10 million expected visitors (Kyodo, 2019, p. 20; Mainichi, 2018).

These are important events that attract extensive media coverage and have substantial societal and political impact. They are therefore worth being properly cyber secured in our digitalized world.

The exponential evolution of Information and Communications Technology (ICT), its ubiquitous nature, the digitalization of BEs such as the Olympic Games or G20 Summits, as well as the increasing implication of mass media in BEs have all added value to these events, as broadcasting become a narrative vector. However, this added value has come at a cost, as the emergence of an increasing number of unsecured devices, programs and applications and an overall lack of cyber-hygiene have engendered new risks and allowed new threat vectors for cyberattacks to develop.

This Trend Analysis (TA) addresses important questions about cybersecurity at BEs, using the G20 Leaders' Summits and the Olympic Games between 2009 and 2019 as a framework:

- What is a BE and what are its various dimensions?
- Are there trends regarding cybersecurity-related organization and processes at BEs?
- What trends can be observed regarding the cyber threat landscape of BEs?
- What does this teach us about current and future cybersecurity at BEs?

In order to answer these questions, this paper starts by addressing the various dimensions of BEs. From this basis, it develops a holistic definition of BEs in Section 2. Section 3 addresses trends observed in relation to G20 Summits and Olympic Games. Section 3.1 highlights organizational challenges of cybersecurity at the G20 Summits and the Olympics, while Section 3.2 and 3.3 present two separate timelines of cyber incidents at G20 Summits and Olympic Games over the period examined. Section 4 analyzes trends and developments in the BE cybersecurity landscape and general challenges of securing BEs. Finally, Section 5 presents conclusions and further considerations regarding cybersecurity at BEs.

This TA is based on an extensive literature review and analysis of a wide spectrum of white papers, journalistic coverage and academic literature. It focuses on BEs themselves rather than on the overall services on which they depend (e.g. transport, IT services, food supply, hotels, etc.). These services are important and need to be addressed in the frame of a bigger research paper.

2 Defining a Big Event

Discussions about “Big Events”, “Mega Events”, or “High-Profile Events”[1] take place in many different forums, ranging from academia to governments, industry, security companies, international organizations, the entertainment industry and so on. Academic literature often comments on such events without defining them. “*Many of us seem to have an intuitive understanding what the term refers to: we know one when we see one*”(Müller, 2015, p. 627). In this regard, the Cannes Festival, the Summer or Winter Olympic Games and the G20 have in common the fact that they have been defined at least once as a Mega Event, Big Event or High-Profile Event.

Before addressing cybersecurity at BEs, it is important to know what exactly needs to be cyber secured: What is a “Big Event”? What terminology should this TA use and why? What kind of conceptualization is best suited to BEs with regard to cybersecurity?

2.1 Conceptualizing a Big Event

For consistency reasons, this TA will use the term “Big Events”, while also referring to “Mega Events” as well as to “High-Profile Events”.

The terminology related to BEs is rather new and only emerged in the academic field from 1987, when the *Association Internationale d’Experts Scientifiques du Tourisme* of Calgary addressed the impact of Mega Events on regional and national tourism development.

Since then, the concept of BEs has often been associated with entertainment, tourism and urbanism. For example, according to Swiss professor Martin Müller, “*Mega Events are ambulatory occasions of a fixed duration that a) attract a large number of visitors, b) have large mediated reach, c) come with large costs […], and d) have large impacts on the built environment and the population*” (2015, p. 629). For other academics, BEs are “*[s]ignificant national or global competitions that produce extensive levels of participation and media coverage and that often require large public investments into both event infrastructure, for example stadiums to hold the events, and general infrastructure, such as roadways, housing, or mass transit systems*” (Mills and Rosentraub, 2013, p. 239).

Another definition comes from the New Zealand Ministry of Business, Innovation & Employment, which states that “*From the government's perspective, a major event is something that: Generates significant immediate and long-term economic, social and cultural benefits to New Zealand. Attracts significant numbers of international participants and spectators. Has a national profile outside of the region in which it is being run. Generates significant international media coverage in markets of interest for tourism and business opportunities*” (Ministry of Business, Innovation & Employment of New Zealand, 2019).

In terms of BEs, both academia and government definitions emphasize the following eight dimensions:

Visitor attractiveness: Prior theories understand BEs as being primarily touristic, with the focus lying on the touristic impact on the host country (Falkheimer, 2008; Müller, 2015). This is particularly true when it comes to sporting events, fairs and concerts, with the Olympic Games between Calgary 1998 and PyeongChang 2018, for example, selling an average of 1.34 million tickets (Gough, 2019). However, tourist attractiveness can differ widely between one BE and another, as BEs such as the G20 Summits are not primarily aimed at attracting tourists.

Cost: This dimension correlates with visitor attractiveness because BEs evidently rely on the infrastructure required for hosting them. Costs are incurred for transport, hotels, venues and other infrastructures for visitors as well as for organizing the BE itself, including temporary jobs and salaries, ICT, infrastructure and security. Here again, costs vary widely between BEs. Indeed, while the Rio 2016 Summer Games cost some €11.62 billion and the 2012 and 2018 FIFA World Cups about €10.3 billion, the 2018 G20 Summit in Buenos Aires cost €98.63 million (Muhanna, 2018; Müller, 2015, p. 631; Reuters Staff, 2017a; Settimi, 2016).

Impact on the host country (urban transformation): This dimension correlates closely with both costs and visitor attractiveness. Indeed, some BEs, for example Olympic Games, have a direct impact on the population as well as on the built environment. Most of the time the infrastructure required for BEs needs to be refurbished or built (conference facilities, stadiums, etc.). Moreover, as aforementioned, the touristic aspect of certain BEs drives the construction or upgrade of roads, hotels, logistics, ICT structures, etc., depending on the event type and size. Most of the time, host countries or cities “*make a strategic use of mega-events to develop infrastructure and push urban renewal, often through leveraging funds that would not be available otherwise*” (Müller, 2015, p. 633). For example, the G20 Summit in Hangzhou allowed the city to boost its tourism as well as develop its infrastructure, even though G20 Summits are not thought of as inherently touristic events (Muhanna, 2018; Z. Zhao, 2016).

Media coverage: Academics agree that “*an unmediated mega-event would be a contradiction in terms*” (Müller, 2015, p. 630). This can be explained as

[1] “*Almost all BEs are also high-profile, i.e. are “known about by a lot of people and receive a lot of attention from television, newspapers, etc.” (Cambridge Dictionnary, n.d.).*

follows: From a societal point of view, mass media is to be considered as a cross-sectoral (social, political, corporate, and cultural) system. At the same time, the generally increased focus on media needs to be seen in the context of a contemporary societal shift led by the quasi-exponential development and ubiquitous nature of ICT. Indeed, media has become as omnipresent as ICT and "*saturates and influences all levels of society, from everyday life (such as the private home) to global institutions (such as the sports industry*)" (Falkheimer, 2008, p. 82).

This global aspect of media is very useful for the countries hosting a BE and for all sectors involved in running it. Indeed, media campaigns and high exposure are likely to impact positively on a host country's image, provided they are well organized and well led: All of the effort a country has gone to in order to host a BE (visitor attractiveness, cost, urban transformation, etc.) is showcased internationally by media coverage. However, any negative observations by the media would be similarly highlighted and could cause reputational damage. Consequently, media coverage of BEs is usually proactively "*integrated into the total place brand strategy*" (Falkheimer, 2008, p. 83).

Moreover, media coverage can differ widely between one BE and another: In the context of entertainment or sporting events, media do not only relay information, but also create entertaining content. As a result, media commercial value (broadcasting rights) can reach in excess of €2 billion (Olympics or FIFA World Cups). However, in the context of international and/or political and/or economic BEs, media would play a more informative and persuasive role.

Size: This TA will, for consistency reasons, consider that an event is big enough to be considered as a BE when it can be categorized as such under both the classifications of Müller (Major, Mega and Giga events) and the New Zealand Department of Business, Innovation & Employment (Major and Mega events) (Ministry of Business, Innovation & Employment of New Zealand, 2019; Müller, 2015, p. 637). However, some events, such as the G20 Summits will still be regarded as BEs, despite their size not fitting either of the above-mentioned categories, because they meet all of the other criteria. Moreover, their political influence is too important to be ignored.

From a strictly technical point of view, however, a large network that needs to be secured is still a network, regardless of whether it relates to the Olympics, the World Economic Forum (WEF) or the G20. The applicable security processes are identical, and only the means used, the visibility of the network and the volume of data involved vary, sometimes exponentially.

Internationality: This dimension, which is particularly important for governmental definitions of BEs (Ministry of Business, Innovation & Employment of New Zealand, 2019), implies both an international audience and international attendees, resulting in the aforementioned mass media coverage. This dimension is the only one which does not differ drastically between one BE and another: The level of internationality, for example, remains the same whether looking at the Olympics or the G20.

Political influence: The literature, when referring to BEs, does not usually address their political dimension. However, this dimension is of considerable importance. First, some BEs, such as the G20 Summits or WEF, are intrinsically political events that provide a platform for discussions between various state and/or non-state-actors at a strategic level. Second, political BEs and also sporting events are directly linked to the notion of "show of force" or "soft power". Indeed, Ravenel describes major sporting events in the following terms: "*It's a geopolitical message: we are a great power because we are able to host a major sporting event. That is the definition of soft power – the ability to assert one's power through means other than military*" (Burnand, 2012, p. 1).

Soft power is closely interrelated with the mediation aspect. Indeed, states often use BEs, regardless of their type, to promote their image or "brand" worldwide through media coverage. Image is central here, because it reflects a nation's "prestige", which in turn is the focus of international affairs theories addressing soft power. Prestige is also considered to be complementary to "traditional material forces" – namely military force (Burnand, 2012; Grix and Houlihan, 2014).

In other words, the act of hosting a BE allows a country to display its cultural, political and foreign policy values as well as its economic power. Indeed, after analyzing sporting BEs, Grix and Barrie concluded that "*Staging sports mega events* … (and BEs in general) … *is, however, more and more about projecting (soft) power and achieving foreign policy goals using non-material means*" (2014, p. 1).

Cross-sectorality and systemic approach: All BEs, whether political, economic or entertainment-oriented, touch on all sectors of society because their organization implementation and conduct draw on all of these sectors (logistics, industry, health, urbanism, economy, politics, security – and in some cases, like the WEF, the Armed Forces). Moreover, from a systemic perspective, the resulting web of synergies affects and is affected by the direct and indirect environment through complex interactions. Applying a systemic logic, the BE and its environment ultimately become one. Here again, the systemic approach of the BEs is a broad and interesting subject that should be analyzed in the frame of a dedicated research paper.

Cooperation and information sharing: This dimension is linked to the cross-sectoral dimension. Organization a BE requires close collaboration and information sharing between the private and public sector, not only in a domestic context, but also between the national and international levels.

2.2 Defining a Big Event

Based on the aforementioned dimensions of BEs, and inspired by Müller's work, a definition of the concept can now be proposed, according to which BEs are: "*ambulatory occasions of a fixed duration that a) attract a large number of visitors, b) have large* (and international) *mediated reach, c) come with large costs […], d) have large impacts on the built environment and population*", e) attract significant numbers of international attendees and spectators, f) exert political influence, and g) have cross-sectoral implications (Müller, 2015, p. 629). The extent to which a particular dimension is expressed in any given BE will differ between events.

3 Cybersecurity at Big Events: Some Examples

Over the last decade, ICT has become ubiquitous and has evolved to such an extent that it is now an enabler of spectacular events. This is true for international fairs, major concerts, sporting events and economic or political meetings alike, all of which rely increasingly on ICT in their overall structure (e.g. timers, security cameras, magnetic or RFID badges, microphones, translators, mobile applications, etc.). These are all examples of "direct ICT", which is immediately responsible for the proper and smooth running of a BE. However, it is important to remember that BEs also depend on extensive "indirect" infrastructure and public providers such as ICT providers, hotels, transportation, etc. that are not being considered here. Both direct and indirect components of BEs have opened the door for new cyber risks and threat vectors.

This section aims to identify the cyber threats associated with BEs by using the evolution of cybersecurity organization processes as a frame and examining timelines of cyber incidents at two major BEs for the period between 2009 and 2019: the G20 Summits and the Olympic Games. A comparative analysis then identifies relevant trends, which are further addressed in Section 4. The Olympics and the G20 Summits are both sufficiently similar and distinctive to extract lessons learned from the full spectrum of BEs.

Section 3.1 explains why cybersecurity is important in BEs and why BEs are important for cybersecurity. Section 3.2 contextualizes the G20 Summits and the Olympic Games, while Sections 3.3 and 3.4 provide an overview of cyber incidents affecting the G20 Summits and the Olympics. Section 3.5 addresses the organizational setup and processes for securing the G20 Summits and Olympics in cyberspace.

3.1 Why Is Cybersecurity Important for Big Events and *Vice Versa*?

Given the range of dimensions impacted by BEs, cybersecurity is a crucial aspect of organizing such events. Indeed, broad media coverage, high investments and the fact that host countries use BEs as geopolitical and soft power platforms make them tempting targets for cybercriminals, hacktivists, and nation-state actors. Accordingly, BE organizers and host countries have too much to lose if they fail to take cybersecurity seriously (i.e. reputational damage, loss of future foreign investments, loss of money already invested, etc.).

However, it is also true that BEs are important for cybersecurity. The organization of Big Events requires close collaboration between a host country's private and public sectors. Similarly, BEs are usually coordinated at both the domestic and international level. The resulting exposure and need to deconflict can constitute good learning opportunities for sharing knowledge, testing risk management infrastructures, and addressing broader security risk factors. The Japanese government, for example, has massively tested and reported on issues of Internet of Things (IoT) security across the entire country in order to provide better security for the 2020 Olympics and respond to the increasing problem of the IoT. BEs can be seen as opportunities to specifically enhance domestic and international collaboration and test in-country crisis response mechanisms, as their organization supports the following:

- Checking national cybersecurity and cyberdefense capabilities, the state of play and landscape in this domain
- Testing national CERTs and their capability to work along with other national and international cybersecurity actors (crisis simulations, risk management exercises, war gaming, etc...)
- Training individuals and companies
- Business opportunities for the private sector, as IT and cybersecurity companies demonstrate their capabilities of addressing the challenges associated with BEs
- Learning: If BE organizers have knowledge-sharing processes in place (e.g. handover-takeover), cybersecurity can be improved with each new event

3.2 Contextualization of the G20 Summits and the Olympic Games

The G20 Summits

Founded in 1999, the G20 or Group of Twenty is an international forum focused on economic and global issues. It contains two tracks: a Leadership track, also called Sherpa track, and a Finance Track. Its membership consists of 19 individual countries[2] and the EU. Other financial entities like the World Bank (WB) and the International Monetary Fund (IMF) also participate (G20, 2019). According to the aforementioned definition of BEs, G20 Summits as well as other high-profile summits represent an investment for host countries, not only in terms of organizational aspects, but also because host cities often take events of this nature as an opportunity to update their infrastructure (Z. Zhao, 2016). This is not always the case, though, due to time and budget constraints. Moreover, the international and political dimension of such events goes hand in hand with a high mediated reach. Even if these events are not meant to attract tourism and are not comparable in size to the Olympic Games, they meet seven of the nine above-mentioned dimensions: cost, impact on the host country (urban transformation), media coverage, internationality, political influence, cross-sectorality, and cooperation and information-sharing.

Since the G20 Summits are highly mediated geopolitical microcosms – consisting in both formal and informal meetings between world leaders – shrouded in a veil of intransparency, they are exposed to a higher level of threat than other high-profile political meetings (Annual and Spring Meetings). Also, the G20 Summits are frequently targeted by espionage campaigns and massive protests on climate change and trade policies, which can also extend into cyberspace (Abedi, 2017; G24, 2019; Kaffenberger, 2018).

The Olympic Games

The modern Olympic Games are leading international sporting events held all over the world, in which a large number of athletes (amateur, professional and top professional) represent their countries in a broad variety of competitions. The Summer and Winter Olympic Games are both held every four years (Young and Abrahams, 2019).

These kinds of BEs are hugely attractive to visitors. For example, the 2016 Summer Olympic Games in Rio de Janeiro boosted the country's tourism to unpreceded levels, with some 6.6 million international tourists visiting Brazil for the occasion (Termèche, 2017). These visitor numbers were, of course, not unprecedented, and it is widely accepted that the Olympic Games are major events due to their substantial size and impressive visitor attractiveness (Müller, 2015). These dimensions impact on the cost of the event, which is necessarily high, and frequently leads to major urban transformation involving the comprehensive mobilization of all societal sectors (cross-sectorality). Moreover, wide media coverage is central to BEs such as the Olympic Games because the associated broadcasting rights are extremely lucrative. Consequently, "*large events are nowadays mediated rather than experienced*" (Müller, 2015, p. 630). Moreover, according to Rid, "*the Olympics have always been the most politicized sporting event of them all*" (Greenberg, 2018). Given the above considerations, the Olympic Games meet all of the aforementioned dimensions for defining a BE.

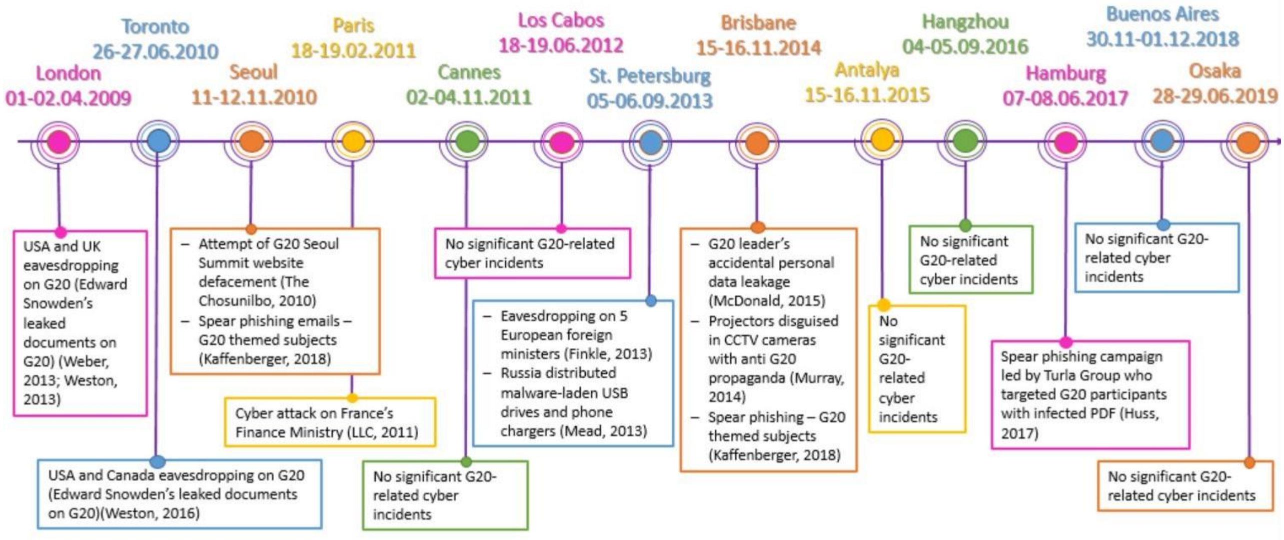
For Greenberg, "*the Olympics have always been a geopolitical microcosm: beyond the athletic match-ups, they provide a vehicle for diplomacy and propaganda, and even, occasionally, a proxy for war*" (Greenberg, 2018). This – and also other reasons that will be addressed below – may be one of the reasons why the Olympics are often targeted in cyberattacks.

[2] List of member countries: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Republic of Korea, Republic of South Africa, Russia, Saudi Arabia, Turkey, United Kingdom, United States of America (USA).

3.3 Cyber Threats to the G20

Diagram 1 shows a timeline of the most notable cyber incidents relating to the G20 to help identify trends.

Diagram 1: Timeline of the most notable G20-related cyber incidents 2009-2019


London
01-02.04.2009
Toronto
26-27.06.2010
Seoul
11-12.11.2010
Paris
18-19.02.2011
Cannes
02-04.11.2011
Los Cabos
18-19.06.2012
St. Petersburg
05-06.09.2013
Brisbane
15-16.11.2014
Antalya
15-16.11.2015
Hangzhou
04-05.09.2016
Hamburg
07-08.06.2017
Buenos Aires
30.11-01.12.2018
Osaka
28-29.06.2019
USA and UK eavesdropping on G20 (Edward Snowden's leaked documents on G20) (Weber, 2013; Weston, 2013)
USA and Canada eavesdropping on G20 (Edward Snowden's leaked documents on G20)(Weston, 2016)
– Attempt of G20 Seoul Summit website defacement (The Chosunilbo, 2010)
– Spear phishing emails – G20 themed subjects (Kaffenberger, 2018)
Cyber attack on France's Finance Ministry (LLC, 2011)
No significant G20-related cyber incidents
No significant G20-related cyber incidents
– Eavesdropping on 5 European foreign ministers (Finkle, 2013)
– Russia distributed malware-laden USB drives and phone chargers (Mead, 2013)
– G20 leader's accidental personal data leakage (McDonald, 2015)
– Projectors disguised in CCTV cameras with anti G20 propaganda (Murray, 2014)
– Spear phishing – G20 themed subjects (Kaffenberger, 2018)
No significant G20-related cyber incidents
No significant G20-related cyber incidents
Spear phishing campaign led by Turla Group who targeted G20 participants with infected PDF (Huss, 2017)
No significant G20-related cyber incidents
No significant G20-related cyber incidents

Before going further into this TA, it is important to note that, because of the highly political and strategic nature of events such as the G20 Summits, most of the literature relating to the actual number and types of cyber incidents that occurred at each summit seems to be classified. It is therefore difficult to exhaustively list all types of G20-related incidents and threats that occurred between 2009 and 2019. Moreover, in contrast to sporting events, studies on the G20 Summits and other comparable events are not publicly available. However, drawing on white papers, newspapers and leaked documents, this TA is able to highlight the fact that almost all cyber incidents associated with G20 Summits between 2009 and 2019 involved espionage.

In early June 2013, Edward Snowden leaked thousands of NSA-classified documents, some of which revealed the following cases of cyberespionage: In April 2009, at the **G20 Summit in London (01-02.04.2009)**, Canada, the UK and the USA allegedly conducted eavesdropping operations on Turkish, Russian and South African officials' G20-related information. Several potential terrorist threats were also countered by intercepting phone calls (phone hacks) and monitoring computers. Then, in June 2010, at the G20 Summit in **Toronto (26-27.06.2010)**, Canada and the USA allegedly again conducted eavesdropping operations on officials' G20-related information by the same means as in 2009 (Weber, 2013; Weston, 2013). No other major cyber incidents were reported for these two events. These cyberespionage cases are likely linked to shifts in the overall geopolitical situation between 2009 and 2010, with the newly elected US President Barack Obama, the Iraq War, the Russia-Ukraine gas dispute, etc.

The **G20 Summit in Seoul (11-12.11.2010)** experienced two major cyberattacks. First, according to the South Korean National Intelligence Agency, the official G20 Seoul Summit website was the target of several defacement attempts in October 2010. The attacks were reportedly attributed to North Korea (The Chosunilbo, 2010). Second, after the Seoul Summit, South Korea detected a spear phishing campaign, which was active throughout January 2011. However, no information on the alleged perpetrators has been made public (Kaffenberger, 2018, p. 10). No other major cyber incidents were reported for that event, although the summit took place during a time of palpable regional tension. Indeed, on 26.03.2010, the South-Korean navy ship Cheonan was torpedoed by North Korea (He-suk, 2018; United Nations Security Council, 2010). It is therefore unsurprising that North Korea would have tried to damage South Korea's image by defacing official websites.

A cyberattack at the **Paris G20 Summit (18-19.02.2011**) related to an espionage campaign and took the form of spear phishing. The attack started in December 2010, before the Paris summit began (Finance Track), and stopped after the end of the summit. Phishing emails and malware attachments were first sent to the French Ministry of Finance and spread to approx. 150 Finance Ministry computers. From there, emails reached the computers of some senior government officials, who forwarded them to other officials. Most of the owners of infiltrated computers reportedly worked on the G20. The main goal of the attack was the exfiltration of classified G20 documents. While there has been no official attribution, some newspapers pointed towards China as being responsible for the attack, because the topics under discussion at the Summit were particularly contentious for China (BBC News, 2011; LLC, 2011). No other major cyber incidents were reported with regards to the Paris G20 Summit.

The **G20 Summits in Cannes (02-04.11.2011)** and **Los Cabos (18-19.06.2012)** were apparently quiet with regards to the cyber domain. Indeed, no major cyber incidents were reported for either of these two summits. The reason for this lull could be that the most sensitive topics, namely the international economy and finance-related issues, had already been addressed by the G20 in Paris.

The **G20 Summit in St. Petersburg (05-06.09.2013)** was exposed to two major cyberattacks. First, according to FireEye, hackers started spear phishing campaigns aimed at European G20 officials and relating to issues including the US military intervention in Syria even before the summit. During the summit, there were eavesdropping campaigns, including phone hacks. No attribution has been officially made, however China was suspected to be responsible for these attacks (Finkle, 2013). Second, during the summit, Russia allegedly distributed spyware-laden USB drives and phone chargers (Mead, 2013). No other major cyber incidents were reported with regards to the summit, which was the first G20 Summit hosted by Russia. The main issues addressed were the global economy and finance, but also the Syrian conflict, Russia-USA relations, including the problem of political asylum for Snowden. These sensitive issues may have motivated various cyberespionage campaigns.

The **G20 Summit in Brisbane (15-16.11.2014)** experienced three major cyber incidents. First, a week before the summit, the Australian Immigration Department accidentally leaked private data of G20 attendees, among them high-profile senior officials, as an email containing the data was sent to the wrong address. The data breach was detected 10 minutes after it occurred (McDonald, 2015). Second, during the summit, a hacktivist group called Dirty Work installed fake CCTV cameras programmed to project activist messages counter to the overall G20 interests. Some fake cameras were found at the last minute, before high-profile personalities such as presidents could see the projected messages (Murray, 2014). Third, prior to the summit, a spear phishing campaign with G20-themed subject lines aimed at seven referenced G20 users was detected. The goal of this campaign was allegedly eavesdropping (Kaffenberger, 2018, p. 10). The most notable issues that may have motivated the second and third incident are the geopolitical themes most urgent at the time, namely the Syrian crisis and the political status of Crimea, which could have led to some tension between Russia and Western countries and to a certain level of cyberespionage.

The **G20 Summit in Antalya (15-16.11.2015)** was apparently quiet with regards to the cyber domain. Indeed, no major cyber incidents were reported in relation to this summit. According to newspapers, the G20 summit in Antalya was so uneventful because of the harsh geopolitical situation at the time, with Paris suffering a series of coordinated terrorist attacks on 13.11.2015, which the Islamic State of Iraq and the Levant (ISIL) claimed responsibility for. On 10.10.2015, a suicide bomb attack was carried out in Ankara, and on 21.10.2015, a Russian passenger airliner was downed in Egypt (Kirton, 2015).

The **G20 Summit in Hangzhou (04-05.09.2016)** was trouble-free, thanks to extensive physical and virtual security measures taken weeks before its start (Geraci, 2016). However, despite the geopolitical turmoil at the time, the summit seems to have been quiet with regards to the cyber domain. Indeed, apart from a single cybersecurity company claiming (most likely for advertising reasons) that the summit experienced massive DDoS attacks, no cyber incidents were reported (R. Zhao, 2016).

The **Hamburg G20 Summit (07-08.06.2017)** was targeted by cyberattacks related to an espionage campaign led by the Turla Group[3]. The associated spear phishing campaign, which sought to elicit G20 attendees' data, began before the summit started and continued through to August 2017 (Huss, 2017).

The **Buenos Aires G20 Summit (30.11-01.12.2018)** was subject to high-intensity protests. However, no cyber incident was reported.

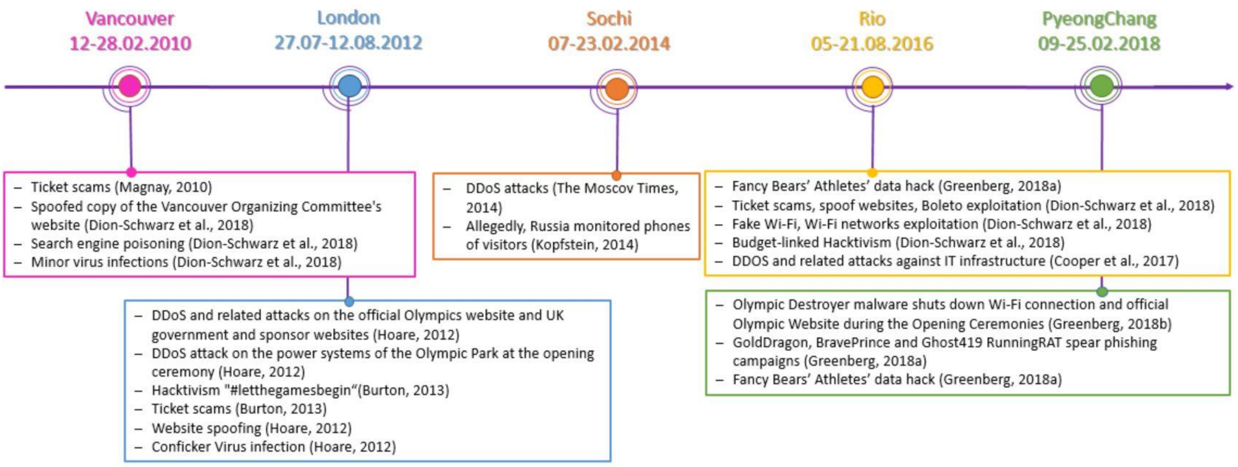
The **G20 Summit in Osaka (28-29.06.2019)** was apparently quiet with regards to the cyber domain. Indeed, no cyber incident was reported for this summit.

3.4 Cyber Threats to the Olympics

Diagram 2 shows a timeline of the most notable cyber incidents related to the Olympic Games 2010-2018 to help identify relevant trends. It is again highly likely that most of the literature indicating the actual number and types of cyber incidents during each Olympics is classified, making it difficult to exhaustively list all types of Olympics-related cyber incidents and threats since 2010. Fortunately, the Olympic Games have been the subject of several studies, which are open

[3] Also called Sofacy or APT28 and allegedly one of the GRU's state-backed group.

Diagram 2: Timeline of most notable Olympic Games related cyber incidents 2010-2018



- Ticket scams (Magnay, 2010)
- Spoofed copy of the Vancouver Organizing Committee's website (Dion-Schwarz et al., 2018)
- Search engine poisoning (Dion-Schwarz et al., 2018)
- Minor virus infections (Dion-Schwarz et al., 2018)

- DDoS and related attacks on the official Olympics website and UK government and sponsor websites (Hoare, 2012)
- DDoS attack on the power systems of the Olympic Park at the opening ceremony (Hoare, 2012)
- Hacktivism "#letthegamesbegin"(Burton, 2013)
- Ticket scams (Burton, 2013)
- Website spoofing (Hoare, 2012)
- Conficker Virus infection (Hoare, 2012)

- DDoS attacks (The Moscov Times, 2014)
- Allegedly, Russia monitored phones of visitors (Kopfstein, 2014)

- Fancy Bears' Athletes' data hack (Greenberg, 2018a)
- Ticket scams, spoof websites, Boleto exploitation (Dion-Schwarz et al., 2018)
- Fake Wi-Fi, Wi-Fi networks exploitation (Dion-Schwarz et al., 2018)
- Budget-linked Hacktivism (Dion-Schwarz et al., 2018)
- DDOS and related attacks against IT infrastructure (Cooper et al., 2017)

- Olympic Destroyer malware shuts down Wi-Fi connection and official Olympic Website during the Opening Ceremonies (Greenberg, 2018b)
- GoldDragon, BravePrince and Ghost419 RunningRAT spear phishing campaigns (Greenberg, 2018a)
- Fancy Bears' Athletes' data hack (Greenberg, 2018a)

source and have been used, along with white papers, to list the major Olympic Games-related cyber incidents between 2010 and 2019.

The cyberattacks on the **Vancouver 2010 Winter Olympic Games (12-28.02.2010)** were relatively limited compared to what the Canadian Government had been expecting. Concerns raised about potential reputational damage as a result of hacktivism as well as about the potential exploitation of the Olympics IT infrastructure (Beaudoin, 2010). However, the following malicious activities were reported: First, on an unspecified date, "*a spoofed copy of the Vancouver Organizing Committee's website, hosted in Ukraine, distributed a video containing codec malware*" (Dion-Schwarz, 2018, p. 30). Second, on an unspecified date, an incident of search engine optimization poisoning with Olympic-themed keywords was discovered, which redirected users to websites which distributed malware. Third, some minor virus infections were reported (Beaudoin, 2010; Dion-Schwarz, 2018). Finally, on an unspecified date, ticket scams were discovered by the Vancouver Organizing Committee. Some 200 ticket accounts were reportedly infiltrated by a Latvian criminal gang (Magnay, 2010). With the exception of the last incident, none were officially attributed.

In anticipation of the **London 2012 Summer Olympic Games (27.07-12.08.2012)**, planners were expecting reputational damage (logistics and human error) as well as cyber threats such as cybercrime, cyberespionage, cyberterrorism and hacktivism (Hoare, 2013). In order to address these risks, London 2012 Olympics planners issued a "30-point cybersecurity action plan". However, on 26.07.2012, an Eastern European hacker group first allegedly probed the Olympics IT infrastructure without detecting any vulnerability. Second, on 27.07.2018, a 40-minute DDoS (botnet) attack was launched on London Olympic Park with some 10 million requests allegedly originating from North America and Eastern Europe. The attack, which was likely intended to disrupt the opening ceremony, failed (Dion-Schwarz, 2018). Third, unknown individuals conducted DDoS and related attacks on the official Olympics and UK government websites as well as sponsor websites (Hoare, 2013). Fourth, on 27.07.2018, hacktivists (#letthegamesbegin) made a call through social media to organize and conduct DDoS attacks on the Olympics. Fifth, a ticket scam campaign started in 05.2012 and continued until the start of the Games. And finally, the Olympics IT infrastructure suffered a virus infection (Conficker) during the construction phase (Burton, 2013).

Planners for the **Sochi 2014 Winter Olympic Games (07-23.02.2014)** were expecting cyber threats like cybercrime, cyberespionage, cyberterrorism and hacktivism, and President Putin launched the so-called *"ring of steel", an extensive security and surveillance cordon surrounding the Olympic Games*" (Andres and Busa, 2014) in order to address these. The Sochi Olympics are also interesting because there is relatively abundant contextualized information available from various sources: On the one hand, Russian media reported that the deputy director of the Russian National Computer Incident Coordination Centre, Nikolai Murashov, declared that "massive DDoS attack" campaigns were conducted against the Olympics website as well as other IT resources as early as on 05.02.2014. According to Murashov, the relevant botnet control centers were located in the USA, Canada, Thailand and Malaysia (The Moscow Times, 2014; Спорт РИА Новости, 2018). On the other hand, there is no corresponding mention of DDoS attack from Western media, which instead emphasized the high risks of Caucasus-related hacktivism (Caucasus Anonymous group) linked to terrorism risks, which did not eventuate (Andres and Busa, 2014; NBC, 2014; Reynolds, 2014). At the same time, Western media described the Sochi security system as so intrusive that privacy issues were raised, particularly with Russia allegedly monitoring visitors' phones and other devices for security reasons (Kopfstein, 2014). Indeed, "*a Russian journalist and security services expert said, everyone should expect* *that all their communications, all the technical devices like smart phones, laptops, will be completely transparent*" (Andres and Busa, 2014).

Another point that makes the Sochi Olympics particularly interesting is that related cybersecurity incidents clearly show the deep link between the Olympics, regional geopolitics (Caucasus conflict) and the overall Russian geopolitical position at the time (alleged Russian state-initiated cyberespionage campaigns against Western countries, especially the USA). These fault lines then found their expression in the Sochi Olympics threat landscape.

The Brazilian government and the **Rio 2016 Summer Olympic Games (05-21.08.2016)** organizers expected cybercrime incidents due to extensive media coverage of and broad interest in earlier Games-related cyber incidents and the Brazilian threat landscape (crime and activism were dominant themes at the time). Unsurprisingly, the cyberattacks on the Rio 2016 Olympic Summer Games took the following forms: "*cybercrime, such as ATM card skimming and point-of-sale malware that can capture and duplicate credit and debit card information. Scams, for example, fraudulent ticket sales for Olympics-related events, as well as fake websites used to collect and steal payment credentials and PII. Fake Wi-Fi networks—some disguised as official Rio 2016 networks—used to collect and steal PII or the exploitation of unsecured Wi-Fi networks. Exploitation of online payment systems, which facilitated the theft of credentials and PII to convert funds into Boletos, a payment method used widely in Brazil, as well as the use of Boleto malware commit fraud. Hacktivist activity in response to budget overruns during the 2014 FIFA World Cup that saw a resurgence in the months leading up to Rio 2016*" (Dion-Schwarz, 2018, pp. 36–37). Another particularly widely publicized incident involved the allegedly Russia-linked APT28 or Fancy Bear group leaking athletes' personal data (medical records) from the World Anti-Doping Association in 09.2016 (Greenberg, 2018). It appears that this was done in response to rumors about the state-organized doping of Russian athletes during the Sochi 2014 Winter Olympics and London 2012 Summer Olympics. The doping allegations were proven to be true in 2017, leading to a number of Russian athletes being stripped of their medals (Gilbert, 2017; Reuters Staff, 2017b, p. 11). Here again, the host country's threat landscape and its geopolitics influenced the cyber threat landscape of the event. Moreover, the dissemination of athletes' data by APT28 during the Rio Olympics highlights that cyber threats can reflect dynamics and conflicts surrounding the Olympic Games themselves.

As shown above, the cyber threats landscape and incidents at the Sochi and Rio Olympics were intimately linked to the host country's geopolitics, and this was also the case at the **PyeongChang 2018 Winter Olympic Games (09-25.02.2018)**. Indeed, McAfee Security identified a spear phishing campaign which they labelled Operation GoldDragon, ahead of the Olympics in January 2018. The campaign had targeted Olympics-related organizations in South Korea since December 2017 and aimed at planting three spyware programs (GoldDragon, BravePrince, and GHOST419). According to McAfee's chief scientist, Raj Samani, the campaign was successful, but it was never officially attributed, even though Samani pointed at North Korean espionage operations (Greenberg, 2018; Sherstobitoff and Saavedra-Morales, 2018). In a separate incident, the Russia-linked group APT28 again and repeatedly leaked data from athletics organizations. Their new campaign started in early September 2017 and was closely linked to the ban of Russian athletes from the 2016 and 2018 Olympic Games. Russian athletes were only able to participate at the PyeongChang Olympics as "OAR", i.e. "Olympic Athlete from Russia". They were neither permitted to wear their colors, nor have their anthem played (Aleem, 2018; Greenberg, 2018).

Finally, the major and most widely publicized incident at the PyeongChang 2018 Olympics was the shutting down of Wi-Fi connections and the official Olympics website during the opening ceremony, which interrupted international broadcasts of the opening ceremony and prevented participants from printing tickets (Liptak, 2018). According to Kaspersky Lab, this incident was caused by the Olympic Destroyer worm, which infected the website pyeongchang2018.com as well as ski station and Atos (IT service provider) network servers. While North Korea and China were initially (and immediately) suspected of having launched the attack, further investigations revealed evidence that Olympic Destroyer was linked to the Russian APT28 (Kaspersky Team, 2018). Once again, this disruption was most likely linked to the ban of Russian athletes from the 2018 Winter Games due to state-sponsored doping.

3.5 Securing BE: What Does This Mean? Examples from the G20 Summits and the Olympic Games

This section highlights the major organizational challenges of protecting BEs against cyberattacks.

The cybersecurity-related organizational challenges of G20 Summits

There is almost no open-source information available on how the cybersecurity of the G20 Summits is organized, although we do know that host countries are responsible for preparing and organizing the series of preparatory meetings and Leaders' Summits in terms of costs, infrastructures, safety, cybersecurity, etc. (Global Affairs Canada-Affaires mondiales, 2019). Limited information about the following organizational aspects of G20 Summits can be gleaned from a small number of newspaper articles and cybersecurity company brochures.

- **Cross-sectoral cooperation and information sharing between government agencies at the domestic and international level**: The Cybersecurity Insiders journal states that, during the Hamburg G20 Summit (07-08.06.2017), the German "IT team" coordinated its efforts with the German police department and the German Federal Intelligence Service. Moreover, the article reports that the USA (CIA and NSA) assisted the German authorities with regard to cybersecurity and cyberdefense (Goud, 2017).
- **Cooperation between the private and public sectors:** According to the Israeli press, on 21.09.2018, the Argentinian defense ministry signed a $5 million contract with its Israeli counterpart to provide cyberdefense and cybersecurity services to the Buenos Aires G20 Summit (30.11-01.12.2018). The package supposedly included *"the implementation of a Cyber Defense Informatics Emergency Response Team (CERT) and a Computer Security Incident Response Team (CSIRT)"* (JTA, 2018).
- According to Guy Rosefelt, director of NSFOCUS[4], the main cybersecurity company responsible for securing the G20 in Hangzhou, that summit was *"considered as a national activity in China, which means companies and government agencies from across China were involved in the process"* (Rosefelt, 2016).
- **Establishment of a temporary cybersecurity network created specifically for the occasion**: For the G20 in Hangzhou, NSFOCUS deployed ten incident response teams that were responsible for securing about 36,000 core assets, including "*web servers, web applications, email servers and databases. It also included communication links between the G20 core institutions and financial institutions, telcos and infrastructure providers*" (Rosefelt, 2016).
- **Early planning and identification of threat actors:** According to NSFOCUS, the company started to prepare six months before the G20 Summit in Hangzhou and deployed a "command and operations center" as well as its own cybersecurity products (e.g. Anti-DDoS Systems (ADS), Web Application Firewalls (WAF), cloud managers, etc.) (Rosefelt, 2016).

This TA therefore concludes that G20 cybersecurity and cyberdefense services are procured in close cooperation between the host country's public and private sectors and international cooperation. In the process, defense ministries (armed forces, intelligence agencies, etc.); interior ministries; institutions responsible for national communication, national cybersecurity and the protection of national infrastructures; industry and the private sector (IT and cybersecurity companies) all collaborate to support the host country's domestic and international interests (including sponsors such as the IMF or the WB, IT companies, etc.).

Given the limited availability of open-source information, this TA cannot address trends in organizing and implementing cybersecurity at G20 events in depth. However, certain conclusions can be drawn from the comparison of and extrapolation from the organization and processes of the Olympics and the limited results obtained from cyber threats to the G20. These are set out further below.

Cybersecurity-related organizational challenges of the Olympic Games

The literature on the organization of cybersecurity at Olympic Games consists primarily of research articles and white papers, which allow a deeper understanding of the main cyber challenges of organizing such events and provide a timeline of events (Section 4.4.). The International Olympic Committee (IOC), and specifically its Digital and Technology Commission, supervises the organization and planning of Olympic Games and gives general guidelines, although host countries do have a degree of freedom. The mission of the Digital and Technology Commission reads as follows:

- *"Ensure that the IOC has an appropriate strategy for the effective, secure and sustainable exploitation of digital and information technologies in support of the activities of the IOC and use of technology in support of the delivery of the Olympic Games and of the Youth Olympic Games*
- *Advise the IOC on priority areas for innovation using digital and information technologies as they emerge*
- *Advise the IOC on its technology supplier strategy*
- *Make recommendations on the IOC's strategy for information security, including cyber-security*
- *Make recommendations on the IOC's cyber incident response and disaster recovery readiness*
- *Advise on approaches to educate and lead the wider Olympic movement in the effective, secure and sustainable use of digital and information technologies"* (IOC, 2019)

This indicates that, in contrast to the G20, the Olympics are more likely to pass lessons learned from past Games on to organizers of future event in order to avoid redundancies and mistakes. The repeated occurrence of similar incidents at subsequent G20 Summits (e.g. spear phishing) suggests a lack of

[4] NSFOCUS is a cybersecurity and IT solutions company.

communication regarding cyber threats, which can be explained by the following hypotheses:

1) There is indeed a lack of knowledge transfer from one G20 event to another because of the highly confidential nature of these events.

2) Lessons learned may be transferred from one G20 event to another, but because of the confidential nature of these events there is no publicly available literature that addresses this transfer of knowledge.

While these two hypotheses require further research, they can be generalized to other political events.

Vancouver 2010 Winter Olympic Games (12-28.02.2010): As early as in 2009, the Canadian government and the IOC were aware of the central role of cybersecurity for the Vancouver 2010 Olympics, and mechanisms to deal with relevant challenges were set up early on: the Royal Canada Mounted Police and Public Safety Canada collaborated to establish the Cyber Security Working Group, which ran three large-scale exercises with regard to the Olympics. Defense Research and Development Canada, the Canadian Computer Incident Response Centre, the Vancouver Games' Security Unit and cyber intelligence experts worked together with key cybersecurity stakeholders to develop a cyber-threat assessment and identify issues to be addressed before the start of the Games, namely "*gaps in Canada's cyber threat situational awareness, siloed planning for cybersecurity threats and responses, and agencies' lack of a coordinated response capability*" (Dion-Schwarz, 2018, p. 29). However, "*information sharing and cross-stakeholder collaboration*" constituted the most critical challenge (Dion-Schwarz, 2018, p. 29). The key cybersecurity lessons learned from the Vancouver Olympics were to plan early on and to first identify and then build strong relationships among public and private stakeholders.

London 2012 Summer Olympic Games (27.07-12.08.2012): The organizers incorporated the lessons learned from the Vancouver Olympics by planning earlier than the Vancouver Olympics planners did, and by implementing a "*multipronged cybersecurity strategy that included a 30-point action plan*" (Dion-Schwarz, 2018, p. 31). The action plan included the Olympic Cyber Co-ordination Team with representatives from the Home Office, the Ministry of Defense, the Security Service/MI5, the Cybersecurity Operations Centre, Government Communication Headquarters and the Centre for the Protection of National Infrastructure (Dion-Schwarz, 2018, p. 32). The Technology Operation Centre was jointly operated by the London Organizing Committee's IT department and experts from Atos, BT and Cisco, and it liaised directly with the Olympic Cyber Co-ordination Team. Experts identified critical infrastructures, including broadcasting structures, with "*the ability to broadcast and the quality of transmission. The spectator's expertise, and UK's reputation*" seen as critical aspects (Dion-Schwarz, 2018, p. 32). Moreover, cybersecurity was integrated into exercises, testing and war-gaming. Key stakeholders from the public and private sectors, such as industry, transportation and public utilities, were coordinated to "*respond quickly, gain buy-in, build trust, disseminate information, and head off cyber threats before they could metastasize*" (Dion-Schwarz, 2018, pp. 32–33). Overall, the cybersecurity organization of the London Olympics was regarded as a success and taken as a model for subsequent Olympics.

Sochi 2014 Winter Olympic Games (07-23.02.2014): There is almost no publicly available information on the cybersecurity organization of the Sochi 2014 Winter Olympics. Apart from Putin's "ring of steel" and massive military deployment, believed to have been aimed at countering Caucasian terrorist and cyberterrorist threats, and the fact that the "ring of steel" comprised a zone around Sochi within which both locals and attendees were subject to near-total surveillance, no organizational information has been leaked. However, it can be assumed that the Russian government took into account lessons learned from the organization and *modus operandi* of the London Olympics (Kopfstein, 2014).

During the **Rio 2016 Summer Olympic Games (05-21.08.2016)**, four teams collaborated to ensure cybersecurity:

- "*Rio2016 CSIRT provided round-the-clock onsite support and handled incidents related to the Rio 2016 infrastructure, phishing attempts targeting official Rio 2016 websites, and websites selling fake tickets.*
- *CERT.br coordinated and facilitated communication with external stakeholders, provided situational awareness, and conducted network monitoring. Incident reporters were encouraged to copy CERT.br on any notifications to Rio2016 CSIRT to support situational awareness.*
- *CTIR Gov, a Brazilian governmental CSIRT, handled incidents that targeted networks belonging to the Brazilian Federal Public Administration.*
- *Centre for Cyber Defense personnel staffed Rio 2016 security command and control centers on a continuous basis, focusing on the defense of critical infrastructure and networks of interest to the Brazilian Ministry of Defense*" (Dion-Schwarz, 2018, p. 38)

PyeongChang 2018 Winter Olympic Games (09-25.02.2018): The PyeongChang organizing committee (POCOG) was particularly concerned about North Korea trying to disrupt the Olympics and, similar to Russia in Sochi, deployed military means to secure the Games. In terms of cybersecurity, the POCOG collaborated with the public sector (Korean National Intelligence Service; Ministry of Culture, Sports and Tourism; Ministry of

Science and ICT; Ministry of Interior; Ministry of Defense; and the national Police Agency). The POCOG ensured that the public sector cooperated very closely with private actors (Korea Telekom, Atos, Ahnlab Security, Akamai, etc.). The POCOG's role was also to connect both private and public-sector actors to the Olympic CERT, which consisted of mainly private-sector experts and was backed by an advisory committee of hacking experts (Oh, 2018). The emphasis was placed on network security (especially broadcasting availability and quality), data security and device security. Moreover, South Korea Telekom deployed a large 5G network throughout PyeongChang. Consequently, both the network and associated devices were better secured than in previous Olympics (ITU, 2018).

4 Trends and Evolution in the Cybersecurity Landscape of Big Events

This section draws on the above timelines of incidents to highlight major trends in the cybersecurity landscape relating to BEs.

Section 4.1 identifies major trends in the cybersecurity threat landscape of G20 Summits. Section 4.2 addresses the same issue with regard to Olympic Games, while Section 4.3 examines trends in cybersecurity-related organizational challenges of both G20 Summits and Olympic Games. Finally, Section 4.4 summarizes the general challenges of securing BEs.

4.1 Trends in the G20 Cybersecurity Threat Landscape

The majority of the reported incidents which occurred during the G20 Summits can be aligned with the following trends:

- Most of the above-mentioned cyber incidents are linked to espionage. Indeed, given the confidential nature of the discussions taking place at G20 Summits and the high profile of participants, these events are very attractive targets for espionage campaigns. In this regard, cyberespionage can be thought as a new means for continuing existing espionage operations
- Most of the cyberespionage attacks are context-related. Indeed, the attacks seem to be closely linked to the geopolitical context of individual G20 Summits (e.g. Syria-related cyberespionage at the G20 Summit in St. Petersburg with spear phishing aimed at European G20 officials referring to issues including the US military intervention in Syria)
- Phishing appears to constitute the primary and malicious USB flash drives the secondary contamination vector (Kaffenberger, 2018).
- Incidents are presumed to be part of state-backed campaigns using non-state actors to spy on G20 attendees
- Most of the incidents seem to start ahead of summits and continue beyond their conclusion. This applies to spear phishing incidents in particular, which need time to spread from the initial infection point to reach the main goals (e.g. Paris and Hamburg)
- Very few DDoS attacks occurred during the G20 Summits addressed in this TA. There may have been more, which may have not been reported by the IT security companies concerned or the mass media

- Only one defacement campaign was reported. Again, other attempts may also have gone unreported.
- Only one hacktivism campaign was reported during the Brisbane G20 Summit.
- More cyber incidents were reported between 2009 and 2014 than between 2014 and 2019. This could point to either of three things: 1) The number of attacks in fact decreased to such an extent that they were not picked up. 2) Attacks were increasingly not reported by mass media. 3) Attacks switched from direct attacks or penetration to man-in-the-middle-type attacks.

Most of the attacks on G20 Summits have a cyberespionage background and are less aimed at disrupting the Summits or at damaging the image of the G20 or host countries. Moreover, considering the political and economic nature of the G20 Summits, more hacktivism would have been expected.

4.2 Trends in the Olympic Games Cybersecurity Threat Landscape

The majority of the reported incidents which occurred during the Olympic Games can be aligned with the trends listed below:

- The most frequently recurring attack vectors used in relation to Olympic Games are DDoS and attacks against IT-related infrastructures, followed by website defacements and ticket scamming
- Most of the ticket scams occurred before the start of Olympic Games to allow the criminals concerned to gather a maximum amount of private visitor data (e.g. credit card information)
- Only one hacktivism campaign was reported, during the 2016 Rio Olympics
- Following the 2014 Sochi Olympic Games and the Russian doping affair, APT28 allegedly hacked athletes' data before, during and after subsequent Olympics. This shows that, like for the G20, cyber threats to the Olympics are not only linked to political and geopolitical backgrounds, but also to the specific political implications of the event
- Only one massive cyberespionage campaign was reported, during the Sochi Olympics, when various Western media stated that Russia collected visitors' personal data in the context of terrorism prevention
- As with the G20 Summits, the political and geopolitical context of the Olympics and their host countries is again important. Indeed, the 2016 Rio Olympics experienced the highest rate of cybercrime. Considering the fact that Brazil already had high rates of cybercrime, it is unsurprising that this increased even further during the Olympics. The 2018 PyeongChang Olympics were another good example, because most of the Games-related attacks allegedly originated in North Korea

Given the scale, visitor attractiveness, cost and mediated reach of Olympic Games, most cyberattacks occurring in this context have a cybercrime background and are aimed at disrupting the Games or damaging the image of the Olympics and their host countries. This is true even though the political component and implications of these criminal cyberattacks and disruption attempts is not to be underestimated.

4.3 Trends in Organizational Cybersecurity Challenges of G20 Summits and the Olympic Games

- Digitalization: As BEs become increasingly digitalized, their organizational cybersecurity aspects and risk landscape have also evolved. Indeed, broadcasting has increased, broadcasting means have evolved, online services have become the norm, the number of connected objects during events (IoT, tablets, smartphones) has grown drastically, and even some measuring instruments used during sporting events are now digitalized and connected to the internet (Cooper et al., 2017). This trend impacts on the organizational aspects of cybersecurity of both the Olympics and the G20
- Cybersecurity management, lessons learned and follow-up: From an organizational point of view, the cybersecurity of Olympic Games evolved between 2010 and 2018 due to information sharing and lessons learned. The cybersecurity organization of the London 2012 Olympics was so successful that it set a benchmark for future Olympics
- Cross-sectoral and multi-level cooperation: Olympic Games are increasingly understood as cross-sectoral events, and their cybersecurity has been increasingly coordinated between not only the public and private sectors but also at the international level and with other non-state actors. This trend is also likely to be true for the organization of events such as the G20 Summits
- Link between geopolitical instability and authoritarian crisis management: Olympics organizing committees take host countries' political as well as geopolitical state of play increasingly into account, and consequently geopolitically less stable host countries are likely to take stronger measures to cyber secure their Games (e.g. the 2014 Sochi or 2018 PyeongChang Olympics). Similar measures

could also be expected for cyber securing G20 Summits.

4.4 General Challenges in Securing Big Events

The sections above have highlighted the trends that cause organizations and host countries to be confronted with the following challenges when securing BEs:

Systemic approach: BEs are complex systems, and complex systems are fragile

According to our definition of BEs, and taking into account their different dimensions referred to in Section 2, BEs are out-of-the-ordinary, high-profile events that incur high costs, attract large numbers of visitors/attendees and extensive media coverage, and are organized through a collaboration between the host country's public and private sectors at both the domestic and international level. The synergies associated with the organization of BEs (joint operations among all sectors, whether domestic or international) are so unique and fragile that they constitute inherent vulnerabilities. Moreover, from a systemic perspective these complex synergies affect and are affected by their direct and indirect environment in a highly complex manner. Applying the systemic approach, the BE and its environment become one, causing a systemic fragility of both the BE and its environment that must not be underestimated.

Identifying threat actors and their motivation/scope

As shown above, BEs can attract a range of threat actors with motivations that vary depending on the nature of the BE concerned and the host nation's political background and geopolitical situation. The challenge here is to foresee potential threats and threat actors, and organization committees have not always been successful in doing so in the past. As a result, they were confronted with unexpected threats.

Table 1 sets out a typology of threat actors and their motivations:

Table 1: Typology of threat actors and their motivations

Threat Actor	Adversary Motivation	Likelihood of occurrence at G20 or Olympics
Foreign intelligence services	Ideology / national interest	Olympics & G20
Cyberterrorists	Ideology / terror / revenge / profit	Olympics & G20
Cybercriminals / Organized crime	Profit	Olympics & G20
Hacktivists	Ideology / revenge	Olympics & G20
Insider threats	Revenge / profit / ignorance	Olympics & G20
Ticket scalpers	Profit	Olympics

Source: (Dion-Schwarz, 2018, p. xiii)

This table summarizes what the above-mentioned G20 Summit and Olympics threat analyses have highlighted: The majority of BEs are confronted with essentially the same threat actors. The decisive point when cyber securing BEs is to be able to understand an adversary's motivation before they attack. This can be achieved only through an in-depth risk assessment that does not fail to contextualize the politics and geopolitics of both the event and the host country.

Adopting a holistic risk assessment framework

For its analysis, this TA borrowed Cooper's risk framework for the cybersecurity of sports, which evaluates "*the ways in which a product can fail and how serious the consequences could be*"(2017, p. 4). This framework integrates three dimensions:

- **Severity**: This dimension "*categorizes attacks based on the degree to which a given incident is likely to impede the event from successfully occurring*"(Cooper et al., 2017, p. 4). The most severe form of attack would cause physical harm to visitors, attendees, athletes, etc., while a less severe attack would merely disrupt an event. The third degree of severity involves attacks against the integrity of an event, and the fourth degree financial loss. Least severe is loss of reputation
- **Occurrence**: This second dimension defines the likelihood of disruption. Physical harm is considered to be unlikely (using cyber tools to cause physical harm is difficult), as is disruption, given adequate backup systems. Financial harm, however, is regarded as likely (especially in case of sporting events). Reputational risks are most likely (Cooper et al., 2017, pp. 4–6)
- **Detectability and nature of an attack**: It goes without saying that a detectable attack will cause less harm because it can be countered in time. Detectability is closely related to the type of attack,

for example, zero-day-type or DDoS-type attacks, which require different levels of investment. The nature of an attack therefore also provides information about the means available to attackers and thus about attackers themselves.

These three dimensions and their sub-dimensions should be calibrated to the specific BE at hand to define the level of acceptable and inacceptable risks.

Implementing a follow-up process

Compared to G20 Summits, Olympic Games have a slightly more centralized organizational structure. Indeed, the International Olympic Committee (IOC) supervises and gives general guidelines for organizing and planning Olympics, even though host countries have a degree of freedom. As a result, there are most likely certain follow-up mechanisms for the Olympics, which facilitate the transmission of knowledge and lessons learned with regard to cyber incidents and cybersecurity, in contrast to G20 Summits.

Organizational processes

Cybersecurity-related organizational processes constitute challenges for both G20 Summits and the Olympics. Important points to be considered by both organizing committees and host countries as they attempt to secure BEs include the following:

- "***Plan early*** *so there is sufficient time to assess event-specific threats, build trust and a community of stakeholders, and establish mechanisms and processes for information sharing, incident reporting, and problem resolution.*
- ***Prioritize cooperation and information sharing****, particularly by drawing in private-sector stakeholders, recognizing that there is no single owner or stakeholder in Olympic cybersecurity.*
- ***Create a shared mission and common cybersecurity goal*** *to help bolster trust and individual stakeholders' openness and commitment to information sharing.*
- ***Establish clear roles and responsibilities among stakeholder****s to help them understand how to support the common goal and respond to specific challenges.*
- ***Incorporate cybersecurity into broader security planning****, training, and exercises right from the start*" (Dion-Schwarz, 2018, p. xii).
- **Include all levels of government in the CERT** to be able to respond quickly top-down but also to be able to tap into some pre-established communities and contacts (bottom-up and top-down).
- **Maintain geopolitical awareness**, namely the capacity of being aware of existing adversaries and their geopolitical interests. As mediated reach is closely linked to media coverage, BE host nations and organizers should be able to address BE-related geopolitical issues to avoid potential reputational, financial or physical harm or event disruption.
- **Organize a handover-takeover system or a follow-up process** in order not to lose lessons learned from previous events and to avoid having to start processes from scratch again.

All of these points need to be understood both as organizational challenges and as means to achieving better cybersecurity at BEs.

5 Conclusion and Further Considerations

Since 2010, the cybersecurity of BEs has evolved and increased along with their digitalization. The most recent developments of ICT, its ubiquitous nature and the complexity it has brought to our societies have transformed the cybersecurity of BEs, as the improvement and proliferation of nefarious cyber capabilities linked to an increasing number of unsecured devices and an overall lack of cyber hygiene add ever greater complexity to cybersecurity at BEs.

In order to provide a better understanding of cybersecurity at BEs, including cybersecurity trends and challenges, this TA first addressed various dimensions of BEs to formulate a comprehensive definition capable of highlighting existing similarities and differences between G20 Summits and Olympic Games.

Regarding the organizational processes associated with cybersecurity at BEs, this TA finds the following: There is a tendency towards increased cybersecurity at BEs, with an emphasis on the cross-sectorality of such events, namely on joint operations between the public and the private sectors, industry, sponsors, etc. International cooperation is an important asset. Moreover, host countries tend to increase cybersecurity to extremes if they are in a tense geopolitical or political situation, for example at the 2014 Sochi Olympics, where press accused the host country of spying on attendees.

The trends identified in the threat landscape of G20 Summits and Olympic Games show that large sporting events are likely to trigger more attacks designed to cause reputational damage to the relevant organization and host country, or cybercrime attacks such as ticket scams, whereas BEs like the G20 Summits are more likely to attract cyberespionage and attacks designed to damage the image/reputation of the host country and/or BE organization. Another interesting point in comparing the evolving threats to both G20 Summits and Olympic Games is that the level of reported incidents at Olympics has remained constant over the years, while incidents at G20 Summits appear to have stopped after 2014.

Media coverage is central for both types of events, and both the Olympics and the G20 use mass media for conveying narratives that are part of the spectacle. Indeed, G20 Summits are largely organized around press conferences and public speeches, and almost half of registered Summit attendees tend to be media representatives (Fordyce and Apperley, 2014). Given that almost every aspect of BEs is linked to mass media, what goes reported or unreported depends on the choice or ability of mass media to draw attention to certain incidents. Regarding the above-mentioned trend of decreasing cyber incidents at G20 Summits, there is consequently the possibility that there has in fact been no such decrease, but that incidents went unreported for whatever reason.

The analysis of the cybersecurity-related organizational aspects and processes of the Olympic Games and G20 Summits as well as their threat landscapes highlights a number of trends and reveals the following considerations, which BE organizers and host countries may wish to take into account in securing BEs:

BEs must be understood from a systemic perspective, especially given that these events depend both directly and indirectly on their surrounding social context, including society and societal sectors, the wider population, etc. Moreover, BEs are likely to have complex effects on their surrounding environment, and these effects can again be direct and/or indirect.

BEs must therefore be conceived of as complex synergies with inherent vulnerabilities which involve both the private and public sectors and are organized at the domestic and international levels. In securing BEs, the aim must be to reduce their complexity in terms of cybersecurity-related organizational processes, or at least to address this issue by planning well ahead. This would provide sufficient time for the private and public sectors to liaise, build trust, create a common goal and distribute clear roles among stakeholders. Moreover, by prioritizing cooperation and information sharing throughout a BE ecosystem increases the likelihood that a holistic, geopolitically aware cybersecurity risk assessment can be conducted. Finally, a handover-takeover system can ensure follow-up of BE cybersecurity management processes and results to facilitate the organization of future BEs.

These considerations apply to BEs in general, as defined in Section 2, and can be therefore be used to support events such as international fairs, large music festivals or the World Economic Forum in Davos[5].

This TA highlights that cybersecurity activities at BEs have increased over the years, as have cyberattacks and their complexity. In view of the continuous evolution of ICT and its ubiquitous deployment in every domain of society, providing cybersecurity for BEs will only become more and more complex, as will the tools required for the task – a trend that is only too evident with regard to the 2020 Tokyo Summer Olympic Games and associated efforts to contain unsecured and unsafe IoT devices (Woollacott, 2019).

[5] Switzerland, however, is a particularly interesting country for organizing BEs because it already has a national culture of tight cooperation between cantons, the private and public sectors, industry and the armed forces.

6 Glossary

Attribution problem: Difficulty to determine with certainty the perpetrator of a cyberattack. Attackers are more difficult to identify because of their ability to cover tracks, perform spoof cyberattacks, or falsely flag other actors as perpetrators (Hay Newman, 2016).

Boleto: Also called Boleto Bancário, this is a payment method used only within Brazilian territory (Novais, 2012).

Cyber hygiene: Analogy to personal hygiene with regard to one's security and practices in cyberspace in order to protect networks and personal computers (European Union Agency for Network and Information Security, 2016).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

False-flag: The act of deceiving an adversary into thinking that a cyberattack was perpetrated by someone else (Pihelgas, 2015).

Hack: The act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Internet of Things (IoT): The IoT is a cyber-physical array of cross-sectoral pervasive network ecosystems which consists of the interconnection via information and communication technologies of multiple connected devices and the data they share. The IoT is regarded as a cross-sectoral and societal phenomenon, as it is present in almost all aspects of daily life and affects all sectors of society (e.g. home automation, the health and entertainment industries, aerospace industry, critical infrastructures, the defense industry, etc.) (Crelier, 2019, p. 6).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Phishing: Technique used to trick a message recipient into disclosing confidential information such as login credentials by disguising messages to suggest that they originate from a legitimate organization (Ghernaouti-Hélie, 2013, p. 437).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Spoofing: The act of usurping IP addresses in order to commit malicious acts such as breaching a network (Ghernaouti-Hélie, 2013, p. 440).

7 Abbreviations

ADS	Anti DDoS Systems
APT	Advanced Persistent Threat
ATM	Automated Teller Machines
BE	Big Event
BEs	Big Events
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
G20	Group of Twenty
ICT	Information and Communications Technology
IoT	Internet of Things
NSA	National Security Agency
OIC	International Olympic Committee
PII	Personally Identifiable Information
POCOG	PyeongChang Organizing Committee for the 2018 Games
TA	Trend Analysis
Telco	Telecommunications company
UK	United Kingdom
USA	United States of America
WAF	Web Application Firewall
WB	World Bank
WEF	World Economic Forum
Wi-Fi	Wireless Fidelity

8 Bibliography

Abedi, M., 2017. G20 protests: Why the international summit attracts so much anger [WWW Document]. Glob. Newsca. URL https://globalnews.ca/news/3576435/g20-summit-why-people-protest/ (accessed 04.07.2019).

Aleem, Z., 2018. Why Russian athletes are marching as “OARs” at the Winter Olympics closing ceremony [WWW Document]. Vox. URL https://www.vox.com/world/2018/2/9/16995270/oar-olympics-russia-country-doping-flag-closing-ceremony (accessed 07.08.2019).

Andres, R., Busa, E., 2014. The Sochi Threat: Russia-U.S. Need to Cooperate on Cyber Terror. The Diplomat.

BBC News, 2011. Cyber attack targeted Paris G20.

Beaudoin, L., 2010. Review and Coordination of Cyber Security for Vancouver 2010, Defense Research and Development Canada Centre for Security Science. ed. CAN, Ottawa.

Burnand, F., 2012. Large sporting events key to soft power [WWW Document]. SWI Swissinfoch. URL https://www.swissinfo.ch/eng/political-games_large-sporting-events-key-to-soft-power/33239944 (accessed 21.06.2019).

Burton, G., 2013. How the London Olympics dealt with six major cyber-attacks [WWW Document]. http://www.computing.co.uk. URL https://www.computing.co.uk/ctg/news/2252841/how-the-london-olympics-dealt-with-six-major-cyber-attacks (accessed 24.07.2019).

Cambridge Dictionary, n.d. high-profile | meaning in the Cambridge Learner’s Dictionary [WWW Document]. URL https://dictionary.cambridge.org/dictionary/learner-english/high-profile (accessed 06.06.2019).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Cooper, B., Chen, K., Feist, Z., Kapelke, C., 2017. The Cybersecurity of Olympics sports: New opportunities, new risks. Center for Long-Term Cybersecurity, Berkeley, CA, USA.

Crelier, A., 2019. Trend Analysis: The Challenges of Scaling the Internet of Things.

Dion-Schwarz, C., 2018. Olympic-caliber cybersecurity: lessons for safeguarding the 2020 games and other major events, Rand. ed. RAND Corporation, Santa Monica, Ca.

European Union Agency for Network and Information Security, 2016. Review of Cyber Hygiene practices. European Union, Heraklion, Geece.

Expo 2015 S.p.A, 2018. Expo Milano 2015 – Official Report.

Falkheimer, J., 2008. Events Framed by the Mass Media: Media Coverage and Effects of America’s Cup Preregatta in Sweden. Event Manag. 11, 81–88. https://doi.org/10.3727/152599508783943273

Finkle, J., 2013. Chinese hackers spied on Europeans before G20 meeting: researcher. Reuters.

Fordyce, R., Apperley, T., 2014. Cyber threats at the G20 (and why they don’t pose much of a risk) [WWW Document]. The Conversation. URL http://theconversation.com/cyber-threats-at-the-g20-and-why-they-dont-pose-much-of-a-risk-33946 (accessed 15.07.2019).

G20, 2019. What is the G20 Summit? | Summit Details [WWW Document]. G20 Osaka Summit 2019. URL https://g20.org/en/summit/about/ (accessed 7.4.19).

G24, 2019. Annual and Spring Meetings | G-24 [WWW Document]. g24.org. URL https://www.g24.org/annual-and-spring-meetings/ (accessed 05.07.2019).

Geraci, M., 2016. How China has re-engineered host city Hangzhou for the G20 summit [WWW Document]. The Conversation. URL http://theconversation.com/how-china-has-re-engineered-host-city-hangzhou-for-the-g20-summit-64710 (accessed 14.08.2019).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Gilbert, S., 2017. In “Icarus,” a Doping House of Cards Tumbles Down [WWW Document]. The Atlantic. URL https://www.theatlantic.com/entertainment/archive/2017/08/icarus-review-netflix/535962/ (accessed 31.07.2019).

Global Affairs Canada-Affaires mondiales, 2019. Canada’s participation at the 2019 G20 summit [WWW Document]. GAC. URL https://www.international.gc.ca/gac-amc/campaign-campagne/g20/index.aspx?lang=eng (accessed 30.08.2019).

Goud, N., 2017. G20 Summit in Germany braces to counter Cyber Attacks. Cybersecurity Insid. URL https://www.cybersecurity-insiders.com/g20-summit-in-germany-braces-to-counter-cyber-attacks/ (accessed 15.08.2019).

Gough, C., 2019. Olympic Winter Games tickets available and sold 1988-2018 | Statistic [WWW Document]. Statista. URL https://www.statista.com/statistics/275219/tickets-available-and-sold-at-the-olympic-winter-games/ (accessed 25.06.2019).

Greenberg, A., 2018. Hackers Have Already Targeted the Winter Olympics—and May Not Be Done. Wired.

Grix, J., Houlihan, B., 2014. Sports Mega-Events as Part of a Nation’s Soft Power Strategy: The Cases of Germany (2006) and the UK (2012). Br. J. Polit. Int. Relat. 16, 572–596. https://doi.org/10.1111/1467-856X.12017

Hay Newman, L., 2016. Hacker Lexicon: What is the Attribution Problem? [WWW Document]. WIRED. URL https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/ (accessed12.01.2018).

He-suk, C., 2018. 'Government looking into ending May 24 measures on NK': Foreign Minister Kang [WWW Document]. URL http://www.koreaherald.com/view.php?ud=20181010000750 (accessed13.08.2019).

Hoare, O., 2013. London 2012: Cyber Security, Sharing our Experiences.

Huss, D., 2017. Turla APT actor refreshes KopiLuwak JavaScript backdoor for use in G20-themed attack [WWW Document]. proofpoint. URL https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack (accessed 17.07.2019).

IOC, 2019. Digital & Technology Commission [WWW Document]. Int. Olymp. Comm. URL https://www.olympic.org/digital-and-technology-commission (accessed 03.09.2019).

ITU, 2018. KT showcases 5G innovation at the Olympics in PyeongChang [WWW Document]. ITU News. URL https://news.itu.int/kt-showcase-5g-olympics/ (accessed 19.08.2019).

JTA, 2018. Israel to provide cyber security to G20 meeting in Buenos Aires. Israelinternationalnews.com.

Kaffenberger, L., 2018. SANS CTI Summit:Cyberthreats to the G20.

Kaspersky Team, 2018. Olympic Destroyer: who hacked the Olympics? [WWW Document]. kaspersky.com. URL https://www.kaspersky.com/blog/olympic-destroyer/21494/ (accessed 12.08.2019).

Kirton, J., 2015. The G20 Antalya Summit's Substantial Success [WWW Document]. G20.Utoronto.ca. URL http://www.g20.utoronto.ca/analysis/151116-kirton-participation.html (accessed 14.08.2019).

Kopfstein, J., 2014. Sochi's Other Legacy.

Kyodo, 2019. Ahead of 2020 Olympics, government to strengthen steps to help foreign visitors in event of massive quake. Jpn. Times Online.

Liptak, A., 2018. Officials confirm that a cyberattack took place during the Winter Olympics opening ceremonies [WWW Document]. The Verge. URL https://www.theverge.com/2018/2/11/17001594/2018-winter-olympics-cyberattack-pyeongchang-opening-ceremonies (accessed 26.07.2019).

LLC, R., 2011. Cyberattack during the Paris G20 Summit [WWW Document]. URL https://www.revolvy.com/page/Cyberattack-during-the-Paris-G20-Summit?smv=24468241 (accessed 16.07.2019).

M. Mills, B., Rosentraub, M., 2013. Hosting mega-events: A guide to the evaluation of development effects in integrated metropolitan regions. Tour. Manag. 34, 238–246. https://doi.org/10.1016/j.tourman.2012.03.011

Magnay, J., 2010. Vancouver Winter Olympics ticket scam a £1.3m write-off.

Mainichi, 2018. National expenditure for Tokyo Olympics set to run 7 times over earlier budget estimate: report. Mainichi Dly. News.

McDonald, political reporter S., 2015. G20 leaders' personal details accidentally made public [WWW Document]. ABC News. URL https://www.abc.net.au/news/2015-03-30/g20-leaders-personal-details-accidentally-made-public/6360148 (accessed 17.07.2019).

Mead, D., 2013. Russia Allegedly Gave Malware-Laden Swag to G20 Delegates. Vice. URL https://www.vice.com/en_us/article/4x3gnw/russia-allegedly-gave-malware-laden-swag-to-g20-delegates (accessed 16.07.2019).

Ministry of Business, Innovation & Employment of New Zealand, 2019. How we define the types of events | Major Events [WWW Document]. URL https://www.majorevents.govt.nz/about/definition-of-a-major-event/ (accessed 25.06.2019).

Muhanna, D., 2018. Fact Sheet: G20 Summit Costs, 2010–2018 [WWW Document]. g20.utotonto.ca. URL http://www.g20.utoronto.ca/factsheets/factsheet_costs-g20.html (accessed 27.06.2019).

Müller, M., 2015. What makes an event a mega-event? Definitions and sizes. Leis. Stud. 34, 627–642. https://doi.org/10.1080/02614367.2014.993333

Murray, D., 2014. Protesters warn of more fake security cameras [WWW Document]. Courr. Mail. URL https://www.couriermail.com.au/news/queensland/g20-protesters-warn-of-more-fake-cameras-in-brisbane/news-story/679c605838b65dd28517021006943c4e (accessed 17.07.2019).

NBC, 2014. Sochi Security: Warning of Cyber Attacks as Hackers Target Games [WWW Document]. NBC News. URL https://www.nbcnews.com/storyline/sochi-olympics/sochi-security-warning-cyber-attacks-hackers-target-games-n22596 (accessed 31.07.2019).

Novais, A., 2012. Boleto Bancário for Beginners [WWW Document]. Braz. Bus. URL https://thebrazilbusiness.com/article/boleto-bancario-for-beginners (accessed 30.08.2019).

Oh, S.J., 2018. Cyber Security of 2018 Pyeongchang Olympic Games.

Pihelgas, M., 2015. Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. NATO Cooperative Cyber Defense Centre of Excellence, Tallinn.

Reuters Staff, 2017a. Rio 2016 price tag rises to $13.2 billion. Reuters.

Reuters Staff, 2017b. IOC bans 11 Russian winter athletes for life for Sochi 2014 doping. Reuters.

Reynolds, M.A., 2014. The Geopolitics of Sochi. Foreign Policy Res. Insititute 8.

Rosefelt, G., 2016. NSFOCUS' Involvement in G20 6.

Settimi, C., 2016. The 2016 Rio Summer Olympics: By The Numbers [WWW Document]. Forbes. URL https://www.forbes.com/sites/christinasettimi/2016/08/05/the-2016-summer-olympics-in-rio-by-the-numbers/ (accessed 25.06.2019).

Sherstobitoff, R., Saavedra-Morales, J., 2018. Malicious Document Targets Pyeongchang Olympics [WWW Document]. McAfee Blogs. URL https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malicious-document-targets-pyeongchang-olympics/ (accessed 12.08.2019).

Termèche, A., 2017. Olympics boosted Brazil to tourism record [WWW Document]. DW.COM. URL https://www.dw.com/en/olympics-boosted-brazil-to-tourism-record/a-37017537 (accessed 29.07.2019).

The Chosunilbo, 2010. Hackers Target G20 Seoul Summit Website [WWW Document]. URL http://english.chosun.com/site/data/html_dir/2010/10/29/2010102900933.html (accessed 7.16.19).

The Moscov Times, 2014. Cyber Attacks on Russian Websites Increasingly Political [WWW Document]. Mosc. Times. URL https://www.themoscowtimes.com/2014/07/09/cyber-attacks-on-russian-websites-increasingly-political-a37174 (accessed 24.07.2019).

United Nations Security Council, 2010. Letter dated 4 June 2010 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the President of the Security Council (S No. 2010/281).

Weber, P., 2013. New Snowden leak: NSA, Britain's GCHQ, eavesdropped on foreign leaders [WWW Document]. URL https://theweek.com/articles/463144/new-snowden-leak-nsa-britains-gchq-eavesdropped-foreign-leaders (accessed 16.07.2019).

Weston, G., 2013. New Snowden docs show Canada let U.S. spy at G20 | CBC News [WWW Document]. CBC. URL https://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448 (accessed 17.07.2019).

Woollacott, E., 2019. In Run-Up To Olympics, Japan Plans To Hack Citizens' IoT Devices [WWW Document]. Forbes. URL https://www.forbes.com/sites/emmawoollacott/2019/01/28/in-run-up-to-olympics-japan-plans-to-hack-citizens-iot-devices/ (accessed 8.21.19).

Young, D., Abrahams, H.M., 2019. Olympic Games | History, Locations, & Winners [WWW Document]. Encycl. Br. URL https://www.britannica.com/sports/Olympic-Games (accessed 29.07.2019).

Zhao, R., 2016. Case Study: Thwarting 100,000+ Attacks on the G20 Summit, the NSFOCUS Experience [WWW Document]. NSFOCUS Inc. URL https://nsfocusglobal.com/case-study-thwarting-100000-attacks-g20-summit-nsfocus-experience/ (accessed 14.08.2019).

Zhao, Z., 2016. G20 summit puts Hangzhou in the global spotlight.

Спорт РИА Новости, 2018. Кибератаки на инфоресурсы ОИ-2014 управлялись из Северной Америки и Азии [WWW Document]. Спорт РИА Новости. URL https://rsport.ria.ru/20181211/1547799246.html (accessed 31.07.2019).

CSS

ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.