CYBER THREAT BRIEF:

2018 Winter Olympics

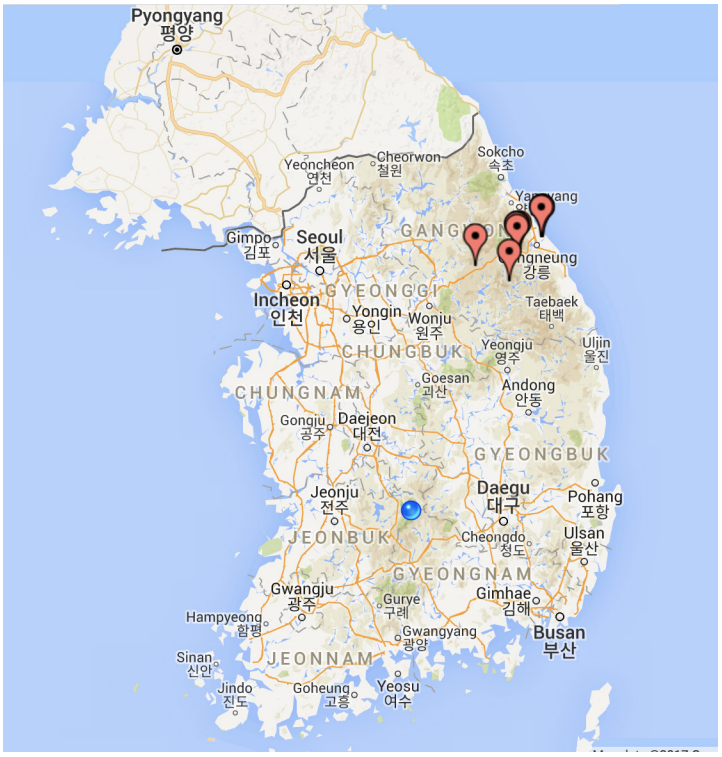
Event	2018 Winter Olympics
Host Country	Pyeongchang, South Korea
Date Start	9th February 2018
Date End	25th February 2018
Website	pyeongchang2018.com sports.or.kr
Social Media	facebook.com/PyeongChang2018 twitter.com/pyeongchang2018 instagram.com/pyeongchang2018 flickr.com/photos/pyeongchang2018_kr youtube.com/user/PyeongChang2018

Executive Summary

There are a number of influences on the 2018 Winter Olympics event that may increase the likeliness of malicious activity. South Korea is technically still at war with North Korea, who has been demonstrably more aggressive in its military posturing over the last year. Despite this, North Korean leader Kim Jung-Un has suggested they might send a team to South Korea for the games. Russia has been banned from participating in the games (although athletes can participate under a neutral flag), causing protest from ordinary Russian citizens. The South Korean deployment of the US THAAD anti-missile system incited Chinese hostility towards South Korea, although relations appear to be back on track. Cross-referencing these geopolitical tensions with notable attacks against Olympic Suppliers highlights similar regions from which malicious activity might occur: Russia, China and North Korea. Hacktivist activity has not been particularly prominent, although the recent activity from Fancy Bear Hack Team and pseudo links to other hacktivist groups might lead to campaigns directed against the IOC and the Olympics in general. There are some boycotts and protests related to the dog and cat meat trade that have created a reasonable amount of interest from animal welfare groups. It is possible that the physical protests might be joined by hacktivists closer to the event. There is the likelihood that the event theme will be used as a phishing lure for opportunistic infections as seen with previous Olympics and other major events.

Key Points

- A direct, transparent, large-scale attack on the Winter Olympics is unlikely.
- Russia may encourage proxy-groups to disrupt the event with low-level attacks because of the decision to ban Russian athletes from participating under the national flag.
- North Korea may use the event to demonstrate power. This might take the form of missile deployment or denial of service attacks.
- Animal welfare groups are likely to stage a protest and/or boycott over South Korea's dog and cat meat trade.
- Executives and other people of interest are at risk of cyber espionage through the use of Hotel Wi-Fi and other forms of unsecured networks.
- There is likely to be an attempt to use the Olympic Event as an opportunistic phishing lure.



Event Details

Event Summary

The Winter Olympics is made up of 95 countries with 6,500 athletes participating in 7 sports and 15 disciplines. The event will take place in two different regions in South Korea; Pyeongchang and Gangneung. South Korea's Defence Ministry will deploy some 5,000 armed forces personnel at the Games. A new Special Weapons and Tactics (SWAT) team has also been created to respond to terror threats. Pyeongchang's organising committee for the 2018 Games (POCOG) is also selecting a private cyber security company to counter cyber threats[1].

Locations

- Pyeongchang Olympics Stadium
- Alpensia Ski Jumping Centre
- Alpensia Biathlon Centre
- Alpensia Cross-Country Centre
- Alpensia Sliding Centre
- Yongpyong Alpine Centre
- Bokwang Snow Park
- Jeongseon Alpine Centre
- Gangneung Hockey Centre
- Gangneung Curling Centre
- Gangneung Oval
- Gangneung Ice Arena

Past Olympic attacks

The Olympics, including the Winter Olympic and the Para-Olympics are major world events and therefore are likely to attract malicious activity in order to capitalize on such a publicized platform. However, these events are heavily monitored and protected with multiple layers of security invested nationally and internationally to ensure safety and security. Since 1970, there have been three fatal attacks categorized as "terror" attacks:

- Munich – In 1972, eleven Israeli Olympic team members were taken hostage and eventually killed by a Palestinian group called "Black September".[2]

1. https://uk.reuters.com/article/uk-olympics-2018-northkorea-exclusive/exclusive-from-cyber-unit-to-troops-south-korea-adds-extra-layer-of-olympics-security-amid-tensions-idUKKCN1C31A5
2. http://www.independent.co.uk/news/world/europe/olympics-massacre-munich-the-real-story-5336955.html

- Atlanta – In 1996, a bomb exploded in the Centennial Olympic park, killing one, by "anti-government extremist" Eric Rudulph.[3]
- Beijing – In 2008, a Chinese man attacked an American couple with a knife killing the man and wounding his wife.

2018 Official Suppliers

The supply chain is a target area for sophisticated espionage campaigns as well as opportunistic criminals. Reasons for this are twofold; the relative impact caused by attacks has increased (due to substantial cloud migration and digitisation), and because a 'weak link' in the chain can help attackers gain access to highly secured upstream networks[4]. The Pyeongchang Winter Olympics website details an official list of sponsors, partners, supporters and suppliers of the event. The following companies are listed as official suppliers for the 2018 Winter Olympics[5]:

Notable attacks on 2018 Olympic suppliers:

- Hanjin Heavy Industries and Construction Co was hit by a cyber-attack in April 2016. The attack left possible classified files exposed. The company's intranet contained sensitive military information including operational manuals of naval war machines[6]. North Korea is suspected[7].
- Hanjin Group is believed to have been targeted by North Korea in a cyber espionage campaign starting in July 2014. Hanjin Group supplies IT management services for Korean Air. The attackers managed to steal files that included information on a medium unmanned surveillance drone and blueprints detailing the design for a US F-15 fighter jet[8].
- KORAIL is believed to have been a victim of a cyber-attack from North Korea in February 2016.

3. https://www.theguardian.com/sport/2016/jul/27/olympic-park-bombings-atlanta-1996-richard-jewell
4. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf
5. https://www.pyeongchang2018.com/en/index
6. http://www.ibtimes.co.uk/north-korea-hand-seen-cyber-attack-south-korea-naval-warship-builder-1559361
7. http://securityaffairs.co/wordpress/47202/hacking/north-korea-defense-contractor.html
8. http://news.softpedia.com/news/north-korea-stole-f-15-jet-blueprints-during-2014-cyber-attack-on-south-korea-505178.shtml

The smartphones of government officials were infected and then used to launch an attack against the rail operator. Seoul suspects it may have been related to threats from Pyongyang regarding joint military exercises.[9] [10]

- In November 2017, Huawei products were found to have rapidly propagated the "Satori botnet" (a variant of the Mirai IoT malware) through the use of a zero-day vulnerability. The vulnerability was found in Huawei Home Gateway routers[11]. A hacker called "Nexus Zeta" is believed to be behind it[12].
- In 2016, Huawei was found to have been working with Boyusec to produce security products that facilitate Chinese intelligence to capture data and control systems. Boyusec is believed to be connected to the MSS (Ministry of State Security)[13] [14]. Boyusec is attributed to APT3[15].
- In 2011, Huawei was banned by the US government from working on the US emergency communications network. The ban is still in effect for any projects of national strategic importance[16].
- Incheon International Airport Corporation was a target of DDoS allegedly by North Korea in 2012. The Reconnaissance General Bureau is believed to have infected games with malware deliberately to infect South Korean users. This botnet was then used to launch an attack against the airport[17].
- In April 2017, it was reported that a Hyundai app had a software vulnerability that left the vehicles susceptible to theft for three months[18].
- Hyundai Merchant Marine was a victim of the Kimsuky campaign reported on in 2013, believed to be operated from out of North Korea.

Analysis of the supply chain risk

Understanding how the suppliers were previously targeted can lend some guidance on how the supply chain might be vulnerable now and in the future. Any actors looking to target the Olympic event may scrutinize previous attacks on suppliers to better understand who might be a weak link. This will allow attackers to be better placed to focus resource and develop plans to conduct attacks. If the Winter Olympics is a target, it is likely that the plan will have been made already and the chosen attack vectors identified. Any infections may already be in place. In a few of the notable attacks identified above, initial infections on unrelated entities were then used to launch attacks on the intended target. Any recently established botnets would fit this pattern from North Korea, who may use the processing power to launch attacks at the intended party. The following actors have been attributed to attacks on some of the Olympic suppliers:

- Kimsuky (North Korea)
- RGB (North Korea)
- APT3 (China)
- Nexus Zeta

9. http://world.kbs.co.kr/english/news/news_Po_detail.htm?No=117399
10. https://www.reuters.com/article/us-northkorea-southkorea-cyber/north-korea-mounts-long-running-hack-of-south-korea-computers-says-seoul-idUSKCN0YZ0BE
11. https://www.crn.com.au/news/massive-satori-botnet-emerges-479522
12. https://www.bleepingcomputer.com/news/security/amateur-hacker-behind-satori-botnet/
13. https://securityboulevard.com/2017/12/chinas-economic-espionage-via-non-attributable-hand/
14. http://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/
15. https://www.bleepingcomputer.com/news/security/chinese-government-contractor-identified-as-cyber-espionage-group-apt3/
16. http://www.nasdaq.com/article/so-who-has-the-most-advanced-cyber-warfare-technology-cm861979
17. http://www.zdnet.com/article/north-korea-ships-malware-infected-games-to-south-korean-users-uses-them-to-launch-ddos-attacks/
18. https://www.reuters.com/article/us-autos-cyber-hyundai/hyundai-app-exposed-vehicles-to-high-tech-thieves-researchers-idUSKBN17R1OF

Geopolitical Tensions

There are a number of geopolitical issues surrounding South Korea and the Winter Olympics.

North Korea

Tension between North Korea and South Korea is at a high at the moment as Kim Jong-Un continues to conduct missile tests despite international sanctions. South Korea is home to many North Korean defectors. A recent North Korean defector who ran across the demilitarized zone was shot with AK rifles as he made his escape, evidencing the use of weapons disallowed under the agreement covering the demilitarized zone. South Korea also takes active measures to monitor North Korea's sanctions evasion efforts, which particularly effects Pyongyang's energy supplies. Ships headed to North Korea carrying oil have recently been seized by the South. These ships were believed to have originated from China. The tension between the North and the South has been cited as a reason for why tickets sales for the Winter Olympics are low[19]. There are concerns that North Korea might seek to provoke or demonstrate its power ahead of the Olympics, and to damage South Korea's image[20]. Despite heightened tensions, direct confrontation is unlikely[21]. More recently, North Korea reached out to South Korea with a proposition to reopen dialogues between the two nations, hinting at a desire to ease military tensions[22].

Russia

The Soviet Union formed the Democratic Republic of Korea (North Korea), with whom South Korea is still at war[23]. The International Olympic Committee (IOC) has banned Russia from participating in the Winter Olympics for alleged doping during the 2014 Sochi Winter Games. This is largely articulated as a national humiliation for Russia, who saw its achievements in the Sochi Olympics as a source of national pride and a defining moment in Putin's presidency[24]. Although athletes can still compete under a neutral flag, ordinary Russians have demonstrated their discontentment through the hashtag #NoRussiaNoGames.

United States

The United States is an ally of South Korea. This is a historic relationship that continues today as evidenced by recent military cooperation; South Korea recently installed US THAAD anti-missile systems and participated in joint military exercises. Although not a direct threat to South Korea or the Winter Olympics, the President of the United States Donald Trump has been unpredictable in his rhetoric towards North Korea. Both Kim Jong-Un and Donald Trump appear to be reactionary to how each other behaves, which generates an uneasy and uncertain foundation for offensive activity. There are also many American athletes that have used their celebrity to protest several issues, including racial inequality and police brutality. The Winter Olympics may be a platform in which athletes may choose to continue to raise their voices.

China

China-South Korean relations deteriorated this year when South Korea decided to deploy the US anti-missile system. China boycotted South Korea's tourism industry and cost the economy 7.5 trillion. China sees the Terminal High Altitude Defense (THAAD) system as a threat to its national security. China has even demonstrably picked on companies like Lotte (who provided land for the system) through fines and closing stores within China[25]. More recently, both countries expressed support for one another by announcing an agreement in October 2017 to put mutual relations back on track. China is South Korea's biggest trading partner despite strong ties to America[26].

Threat Landscape

Physical Protests/ Boycotts

There are a few areas of controversy that seem to dominate potential protest activity. The most frequently mentioned issue is around South Korea's dog and cat

19. http://fortune.com/2017/09/12/no-ones-buying-tickets-to-the-winter-olympics/
20. http://theweek.com/articles/737300/north-korea-planning-something-big-2018-olympics
21. https://www.ijet.com/content/special-report-attacks-xxiii-olympic-winter-games-pyeongchang-south-korea-unlikely-despite
22. https://www.nytimes.com/2018/01/02/world/asia/south-north-korea-olympics-talks.html
23. https://www.fpri.org/article/2017/11/nuclear-weapons-russian-north-korean-relations/
24. https://www.theguardian.com/sport/2017/dec/10/russia-reaction-winter-olympics-ban-sochi-2014-putin-mutko
25 https://qz.com/1149663/china-south-korea-relations-in-2017-thaad-backlash-and-the-effect-on-tourism/
26. https://thediplomat.com/2017/11/south-korea-and-china-make-amends-what-now/

meat trade. Animal welfare groups have set up a few petitions and boycott pages to foster protest.

Protests/Boycotts:

- Boycott PyeongChang 2018 Winter Olympics in South Korea, A Dog Eating Nation![27] [28]
- Kontinental Hockey League has suggested it may withdraw its players from the Pyeongchang Olympics in protest of doping investigations into Russian athletes[29].
- Russia's Bosco, the exclusive supplier of clothing to the International Olympic Committee from next year, will ask the IOC not to use its brand at the 2018 Winter Olympics[30].
- Twitter campaign #NoRussiaNoGames linked to Russian state owned Twitter bots[31].
- Although not a boycott, the NHL will not participate in the PyeongChang 2018 Winter Olympics[32].

Social Media:

The table below reflects one week of social media mentions using keywords that include "Winter Olympics" and an optional mixture of protest related keywords. The selection shown are those that have "interacted" the most. The data shows that the most interactive handles appear to be specifically interested in animal welfare.

Handle	Followers	Interest	Reach	Interactions
@ForAnimals1313	240	Animal Rights, Animal Welfare, Cambodia, Dogs, Michael Kors	16,447	69
@RotenbergBros	70	Chernobyl, Google, Trader Joe's, Ukraine, Vehicles	6,932	51
@SeaDolphinLove1	1,192	Animals, Cats, Dogs, Ecology, Wildlife	61,932	33
@heavenlydogz	2,206	Animal Rights, Animals, China, Dogs, South Korea	70,739	29
@mojgan_re	358	Animal Welfare, Cambodia, Dogs, Humane Society, Petsmart	101,787	28
@kellskelsner	325	Animal Rights, Animal Welfare, Dogs, Pets, Ricky Gervais	8,116	25
@Cat_Kapow	2,813	Animal Welfare, Animals, Cats, China, Dogs	68,851	24
@_Pehicc	6,526	Animal Rights, Animal Welfare, Animals, Cats, Dogs	137,130	21
@oimaco8	2,887	Animal Rights, Animals, Cats, Dogs, Dolphins	90,065	20
@argentomaris1	1,857	Animal Rights, Animal Welfare, Animals, China, Dogs	39,768	18

27. https://www.change.org/p/boycott-pyeongchang-2018-winter-olympics-in-south-korea-a-dog-eating-nation
28. http://www.koreank9rescue.org/2017/11/07/korean-activists-protest-outside-of-gupo-market/
29. https://www.si.com/olympics/2017/11/04/khl-may-pull-out-olympics
30. https://www.reuters.com/article/us-olympics-2018-russia-bosco-ioc/russias-bosco-wants-brand-disassociated-from-winter-olympics-idUSKBN1EE23P
31. https://www.reuters.com/article/us-twitter-russia-olympics/norussianogames-twitter-bots-boost-russian-backlash-against-olympic-ban-idUSKBN1E223V
32. https://www.nhl.com/news/nhl-will-not-participate-in-2018-winter-olympics/c-288385598

Hacktivist

Overall hacktivist activity in South Korea is low. There is limited information regarding planned hacktivist activity for the Winter Olympics, however some activity has been seen originating from China:

- The PyeongChang Winter Olympics website was defaced. China is believed to be behind it in retaliation for the deployment of US THAAD anti-missile defense system. The defacements are designed to boycott the company Lotte, and therefore resemble hacktivist activity. A number of organisations were defaced at the same time, including the Seoul Metropolitan Government and the World Taekwondo Championships[33]. Lotte Duty Free website was also struck by a denial of service attack allegedly for the same reasons[34].

The present issues related to Russia's ban from the Winter Olympics by the IOC has attracted activity from Fancy Bears' Hack Team. During 2017, the group coordinated activity in order to leak information about corruption. The Twitter campaigns and embarrassment for Russia provide some evidence of grievance that might call for a potential targeting of the Winter Olympics.

Past Olympic hacktivist activity has been evident where controversy has been part of the Olympic decision-making process. In Brazil hacktivists took part in campaigns under the hashtag #OpOlympicsHacking because of civil unrest and strong anti-government sentiment[35].

APT and Organised Crime

Cybercrime is a threat in tourist areas and is likely to increase during high profile events[36]. Scams and phishing using the Olympic theme were seen in previous years. One example of this includes phishing lures promising access to live streaming of the events.[37]

A global event attracting a number of high-profile individuals is a prime opportunity to take advantage of any holes in an individual's operational security. There are a number of risks to travelling executives and persons of interest. The event hosts people from all over the world, therefore multiple agencies and groups will be able to take advantage of information stealing opportunities. Officials have alerted travelers to the risk of cyber espionage in previous games[38]. Because of the multiplicity of the issue it is difficult to pinpoint exact interest, however the following groups are of particular interest due to activity in and around South Korea and/or travelers to the Winter Olympics:

- Russian APT28 reportedly targeted hotel Wi-Fi in August 2017[39]
- Dark Hotel APT continues to target business

33. http://www.koreatimes.co.kr/www/tech/2017/03/133_225311.html
34. http://english.yonhapnews.co.kr/national/2017/03/02/0301000000AEN20170302010651320.html
35. https://www.opendemocracy.net/digitaliberties/robert-muggah-nathan-b-thompson/with-anonymous-latest-attacks-in-rio-digital-games-have-begun
36. https://www.flashpoint-intel.com/blog/bri/risks-international-travel/
37. google search: site:phishtank.com "olympics" shows entries for the RIO Olympics in August 2016
38. https://www.usatoday.com/story/news/world/2016/06/28/olympics-hacking-rio/86296084/
39. https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

travelers in luxury hotels [40] [41]

- Lazarus – North Korean financially motivated attacks against bitcoin exchanges and financial institutions [42] [43]
- China – two Chinese APT groups have been targeting the US THAAD anti-missile system recently deployed in South Korea, including APT10[44]

Conclusion

There is a mixture of issues that arguably will have an influence whether the Winter Olympics 2018 is at risk of any cyber activity or physical threats. The consequence of a large-scale attack will invariably be somewhat grand in scale too; there will be sophisticated and well-orchestrated security teams from all over the world looking after the event. Countries like Russia and North Korea both have cause to try and disrupt the event or embarrass the host and organizers. However, the question is whether they will do so and to what extent if they do. Both countries are able to demonstrate power or to initiate malicious activity through indirect means. Denial of service, pseudo-hacktivist activity, military maneuvers and demonstrations of offensive capability might be more likely. There might be more of a risk of cyber-espionage to individual executive travelers or people of interest who could be lured by opportunistic phishing campaigns and through the use of unsecured Wi-Fi networks.

40. https://labs.bitdefender.com/2017/07/inexsmar-an-unusual-darkhotel-campaign/
41. http://www.zdnet.com/article/hackers-are-using-hotel-wi-fi-to-spy-on-guests-steal-data/
42. https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new
43. https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spear-phishing
44. http://securityaffairs.co/wordpress/58226/cyber-warfare-2/china-targeted-south-korea-thaad.html