Working Paper 11/2021
4 October 2021

The 19th of July: divided or united in cyberspace? From the EU and NATO to Five Eyes and Japan

Stefan Soesanto

The 19th of July: divided or united in cyberspace? From the EU and NATO to Five Eyes and Japan

Stefan Soesanto | Senior Cyber Defence Researcher at the Center for Security Studies (CSS) at ETH Zurich | @iiyonite

Index

Summary

The coordinated public attribution campaign by the EU, NATO, Five Eyes and Japan on 19 July 2021 has been portrayed as a largely coherent effort of like-minded countries confronting China's malicious cyber activities. As this Working Paper will show, this was the case neither in substance nor in form. For instance, while the Five Eyes are the most coherent group when it comes to public attribution, confronting Beijing on the MS Exchange campaign, and highlighting APT40 activity, they failed to achieve consensus on denouncing Beijing's use of 'criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit'. Similarly, given the absence of high-volume and high-profile APT40 activity in Europe, it should come as no surprise that the majority of NATO and EU member states were relatively muted on the issue. Meanwhile, the Japanese government –for the first time ever– put forward its own public attribution assessment on APT40. Based on the public information available as of the time of writing, this Working Paper aims to disentangle and explain what occurred on 19 July. To the author's knowledge this is the first ever case study to take a deep look into a coordinate attribution campaign. It brings together an in-depth analysis of the various government statements and a database that tracked the social media behaviour of numerous government ministries on 19 July 2021.[1]

[1] See the database here.

(1) Introduction

On 19 July 2021 the EU's High Representative for Foreign Affairs and Security Policy (HR), Josep Borrell, published a Declaration on behalf of the EU urging the 'Chinese authorities to take action against malicious cyber activities undertaken from its territory'.[2] The HR's Declaration kicked off a host of other government statements and tweets on that day, encompassing a wide range of different attribution assessments, intelligence assertions, strategic objectives and diplomatic support. Coordinated to a degree by Washington, the flurry of statements by the EU, NATO, Five Eyes and Japan on Chinese cyber activities was perceived by numerous media outlets as one coherent narrative with a few subtle discrepancies. The goal of this Working Paper is to break that narrative apart by contextualising government motivations and disentangling the political intricacies that were on display that day.

(2) The EU

Since the introduction of the EU's Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities on 19 June 2017 (the so called 'cyber diplomacy toolbox'), the EU's HR has made six Declarations (excluding the Declarations on EU cyber sanctions).[3] They include a Declaration on respect for the rules-based order in cyberspace (12 April 2019), a call for responsible behaviour after the cyber-attacks against Georgia (21 February 2020), on malicious cyber activities exploiting the coronavirus pandemic (30 April 2020), to promote international security and stability in cyberspace (30 July 2020), on expressing solidarity with the US on the impact of SolarWinds (15 April 2021) and the most recent one on malicious cyber activities undertaken from Chinese territory (19 July 2021).[4]

None of the Declarations by the HR fall into the category of public attribution, as (a) an HR Declaration speaks on behalf of the EU and all the 27 members states, and (b) there is no mechanism for collective public attribution at the EU level. The reasons for this setup are manifold, including inequalities between member state attribution capabilities, an unwillingness to share classified intelligence with all the other 26 national governments and a desire to maintain national sovereignty over foreign, security and

[2] Council of the EU (2021), 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory', concilium.europa.eu, 19/VII/2021.

[3] Council of the EU (2017), 'Cyber attacks: EU ready to respond with a range of measures, including sanctions', consilium.europa.eu, 19/VI/2017.

[4] Council of the EU (2019), 'Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace', consilium.europa.eu, 12/IV/2019; Council of the EU (2020), 'Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace', consilium.europa.eu, 21/II/2020; Council of the EU (2020), 'Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic', consilium.europa.eu, 30/IV/2020; Council of the EU (2020), 'Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace', consilium.europa.eu, 30/VII/2020; Council of the EU (2021), 'Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation', consilium.europa.eu, 15/IV/2021; and Council of the EU (2021), 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory', consilium.europa.eu, 19/VII/2021.

defence issues. In essence, there are clear EU institutional limitations on what the HR can say on behalf of the Union, which explains the Declaration's natural focus on norms and international law.

In terms of the timeline, we can presume that the deliberations on the HR publishing a Declaration on Chinese cyber activities were likely discussed within the EU Council's Horizontal Working Party on Cyber Issues (HWPCI) under the agenda item 'Cyber diplomacy Toolbox: Discussion', between 28 June and 13 July 2021.[5] Unlike EU cyber sanctions –which are deliberated upon in the HWPCI, forwarded for agreement to the Council's Working Party of Foreign Relations Counsellors (RELEX) and then voted on in the Council's Permanent Representatives Committee II (COREPER II)–, a Declaration only needs to find agreement within the HWPCI and is then adopted by the Council through a silent written procedure. This implies that the institutional turnaround for a Declaration is far quicker and far less bureaucratic than adopting EU cyber sanctions for instance.

Analysing the Declaration of 19 July 2021, the first item that draws attention is that it mentions the compromise and exploitation of Microsoft Exchange Servers.[6] According to the Declaration, this activity 'undermined the security and integrity of thousands of computers and networks worldwide, including in the member states and EU institutions', and 'allowed access to a significant number of hackers that have continued to exploit the compromise to date'.[7] Notably, while Microsoft's Threat Intelligence Center 'attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China', the HR's Declaration does not mention Hafnium a single time, nor does it specifically identify the collusion between the Chinese state, hackers-for-hire and the criminal eco system, which was at the heart of the normative breakdown in the MS Exchange campaign.[8] Instead, the Declaration keeps a cautious distance by talking about 'malicious cyber activities to have been undertaken from the territory of China', and thus urges the Chinese authorities to adhere to international law and 'not allow its territory to be used for malicious cyber activities'.[9]

As of the time of writing, it is unclear how many systems and organisations located within the EU's territory were actively targeted by the four 0-days used in the MS Exchange Server campaign (CVE-2021-26855/CVE-2021-26857/CVE-2021-26858/CVE-2021-27065), and how many were accessed through the China Chopper web shell that was

[5] Council of the EU (2021), 'Notice of Meeting and Provisional Agenda - Horizontal Working Party on Cyber Issues', CM 3780/21, 25/VI/2021; Council of the EU (2021), 'Notice of Meeting and Provisional Agenda - Horizontal Working Party on Cyber Issues', CM 3989/21, 12/VII/2021.

[6] Brian Krebs (2021), 'A basic timeline of the exchange mass-hack', Krebsonsecurity, 8/III/2021, https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/.

[7] Council of the EU (2021), 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory', concilium.europa.eu, 19/VII/2021.

[8] Microsoft Threat Intelligence Center (2021), 'HAFNIUM targeting Exchange Servers with 0-day exploits', Microsoft, 2/III/2021; Andy Greenberg (2021), 'How China's hacking entered a reckless new phase', Wired, 19/VII/2021.

[9] Council of the EU (2021), 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory," concilium.europa.eu, 19/VII/2021.

left behind by Hafnium as a means to maintain a foothold in the system.[10] The Executive Summary of CERT-EU's Threat Landscape Report Q1 2021 mentions seven significant incidents that affected EU institutions, bodies and agencies, of which two were 'related to the global Microsoft Exchange ProxyLogon exploitation' (CVE-2021-26855 & CVE—2021-27065).[11] One of the EU agencies was the European Banking Authority, which acknowledged on 7 March 2021 that it had 'been the subject of a cyber-attack against its Microsoft Exchange Server', and as a precautionary measure 'decided to take its emails systems offline'.[12] The second EU institution, body or agency affected by ProxyLogon is currently still unknown.

The most important item the HR's Declaration touches upon is that the EU member states 'detected malicious cyber activities with significant effects that targeted government institutions and political organisations in the EU and member states, as well as key European industries. These activities can be linked to the hacker groups known as Advanced Persistent Threat 40 and Advanced Persistent Threat 31 and have been conducted from the territory of China for the purpose of intellectual property theft and espionage'.[13] This means that the EU member states not only shared the intelligence threat at the EU level but that they also allowed the HR to explicitly link those activities to APT40 and APT31.

APT40 is a Chinese threat actor who according to FireEye has been active since at least 2013.[14] In January 2020 the group was publicly outed by Intrusion Truth, which connected a network of individuals, job adverts, QQ accounts and front companies to Hainan University and the Hainan Department of the Chinese Ministry of State Security.[15] Notably, APT40 has not made it into the European news cycle when it comes to specific targets within EU territory. The only smaller item on APT40 activity in Europe was published by FireEye in a threat research blog post in March 2019.[16] According to FireEye, APT40 conducted campaigns targeting universities involved in naval research and targeted organisations in countries that are strategically important to China's Belt and Road Initiative. Targets in Europe included two EU countries (Germany and Belgium), two non-EU NATO countries (the UK and Norway) and Switzerland. From the APT40 US Grand Jury indictment released on 19 July 2021 we know that APT40 targets an unnamed 'German industrial conglomerate with hundreds of subsidies around the

[10] Microsoft Threat Intelligence Center (2021), 'HAFNIUM targeting Exchange Servers with 0-day exploits', Microsoft, 2/III/2021; Joshua Deacon (2021), 'HAFNIUM, China Chopper and ASP.NET Runtime', Trustwave – SpiderLabs Blog, 15/III/2021.

[11] CERT-EU (2021), 'Threat Landscape Report - Q1 2021 Executive Summary', media.cert.europa.eu, 30/VII/2021.

[12] EBA (2021), 'Cyber-attack on the European Banking Authority', eba.europa.eu, 7/III/2021.

[13] Council of the EU (2021), 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory', concilium.europa.eu, 19/VII/2021.

[14] Fred Plan *et al*., 'APT40: Examining a China-Nexus Espionage Actor', FireEye Threat Research Blog, 4/III/2019.

[15] Intrusion Truth (2020), 'Who else works for this cover company network?', intrusiontruth.wordpress.com, 13/I/2020; Intrusion Truth (2020), 'APT40 is run by the Hainan department of the Chinese Ministry of State Security', intrusiontruth.wordpress.com, 16/I/2020.

[16] Fred Plan *et al*. (2019), 'APT40: Examining a China-Nexus Espionage Actor', FireEye Threat Research Blog, 4/III/2019.

world'.[17] There is no information included in the indictment as to which company, organisation or university APT40 targeted in Belgium.

APT31 (or Zirconium) is a Chinese threat actor who according to Positive Technologies has been active since at least 2016.[18] In September 2020, Microsoft reported that APT31 'attempted to gain intelligence on organizations associated with the [2020] US presidential election'.[19] And earlier this year, CheckPoint uncovered that APT31 stole and exploited in the wild an unknown Equation Group 0-day (also known as the NSA's Tailored Access Operations unit).[20] In Europe, APT31 most prominently entered the news cycle in February 2019 with reports that the Norwegian software firm VISMA was hacked.[21] While Recorded Future attributed the activity to APT10 and the Cloud Hopper campaign, Microsoft's Ben Kohl noted that the registered C2 domains were clearly Zirconium.[22] The attribution conundrum remained unresolved until 17 June 2021, when Norway's Police Security Service (PST) attributed the 2018 breach of the Norwegian government's administration system to the same threat actor that breached VISMA.[23] Earlier that day, the Head of Counterintelligence at PST, Hanne Blomberg, revealed in an interview with NRK that APT31 was behind the operation against Norway's government administration systems.[24] Within the individual EU member states, Germany's Federal Office for the Protection of the Constitution released a security advisory in January 2021, warning against an ongoing APT31 campaign targeting political institutions in Germany and the West.[25] And in March 2021 the Finnish Central Criminal Police (KRP) and the Finnish Security Intelligence Service (SUPO) attributed the breach of the Finnish Parliament's internal IT system in the autumn of 2020 to APT31.[26]

Interestingly, the EU Council accidentally disclosed to me in a freedom of information request an EU classified slide show dated January 2019 from the Signals Intelligence

[17] United States District Court, Southern District of California (2021), 'United States of America v. Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin, and Wu Shurong', November 2019 Grand Jury, filed on 28/V/2021, p. 6.

[18] Positive Technologies (2021), 'APT31 new dropper. Target destinations: Mongolia, Russia, the US, and elsewhere', PT ESC Threat Intelligence, 3/VIII/2021.

[19] Tom Burt (2020), 'New cyberattacks targeting U.S. elections', blogs.microsoft.com, 10/IX/2020.

[20] Eyal Itkin & Itay Cohen (2021), 'The Story of Jian – How APT31 Stole and Used an Unknown Equation Group 0-Day', CheckPoint Research, 22/II/2021.

[21] Jack Stubbs (2019), 'China hacked Norway's Visma to steal client secrets – investigators', Reuters, 6/II/2019.

[22] Ben Kohl (2019), 'This activity is not APT10. It is all APT31 (or ZIRCONIUM) in our terms. The C2 domains that you mention were all registered and the threat actors made subsequent changes in specific ways that we attribute (with other information) to ZIRCONIUM', Twitter, 6/II/2019.

[23] Dafina Shala (2021), 'Etterforskningen av datanettverksoperasjonen mot statsforvalterembeter henlegges', PST, 17/VI/2021.

[24] Øyvind Bye Skille *et al*. (2021), 'For første gang sier PST at Kina står bak et dataangrep', NRK, 17/VI/2021.

[25] Bundesamt für Verfassungsschutz (2021), 'BfV Cyber-Brief Nr.01/2021 – Hinweis auf aktuelle Angriffskampagne', verfassungsschutz.de, 18/I/2021.

[26] Poliisi (2021), 'Eduskunnan tietojärjestelmiin kohdistuneen tietomurron tutkinnassa selvitetään yhteyttä APT31-toimijaan', poliisi.fi, 3/III/2021; SUPO (2021), 'Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi', supo.fi, 18/III/2021.

Analysis Capability (SIAC) within the EU's Intelligence and Situation Centre (INTCEN).[27] INTCEN serves as the EU's 'hub for situational awareness and threat assessments on cyber issues' and deals with 'voluntary intelligence contributions from the member states'.[28] Slide six shows a 'China related APT map' on which APT10 and APT31 are put together in a dotted box. This likely visualises the attribution conundrum surrounding Norway's VISMA. Overall, the map shows a total of 19 different Chinese APT actors, but notably absent from the list is APT40.

Taking in all this information, we can deduce that APT31 activity is of imminent importance to the EU and most of the member states, while APT40 activity is of less or even no relevance in a European context. Notably, on 21 July 2021 –two days after the coordinated attribution campaign–, France's ANSSI put out an alert stating that it 'is currently handling a large intrusion campaign impacting numerous French entities. Attacks are still ongoing and are led by an intrusion set publicly referred as APT31'.[29] If we assume that the public attribution campaign to call out Chinese cyber activities on 19 July was coordinated by the US, then the APT40 inclusion in the HR's Declaration seems likely to be a nod to the US Department of Justice charging four APT40 members on that day. However, given the imbalance in priorities one would expect that APT31 would at least be mentioned in a normative context by any of the Five Eyes members (apart from the UK), NATO or even Japan. Yet none of them cared enough to mention APT31 even once. From the outside looking in, it seems that the coordination on this attribution campaign was rather one sided.

If we go a step further and look at the tweets and retweets on the official government Twitter accounts of each individual EU member state (Ministries of Foreign Affairs and Permanent Representations to the EU), we can somewhat statistically analyse whether the HR's Declaration positively resonated with the member states, whether some member states did not really care for the Declaration, and whether there were significant outliers.[30]

Of the 27 EU member states, nine remained completely silent on the HR's Declaration, 14 posted a tweet in support and four simply retweeted the EU Council's Press tweet of the Declaration with no comment whatsoever (Croatia, France, Germany and Ireland). Two member states reacted positively: Estonia and Romania. The Estonian Ministry of Foreign Affairs retweeted the HR's Declaration and the NATO declaration (which we will look at next), but also released its own supporting attribution statement that links China's Ministry of State Security to the Microsoft Exchange Server campaign –echoing the Five

[27] Stefan Soesanto (2021), 'Today is a very good day :) FOI request was partially successful. It includes: (1) A 2019 Slide deck from the EEAS Intelligence and Situation Center (INTCEN) on APT10 (HWP brief) Q: APT8 and APT20 circled? Q: Previous (EU?) diplomatic attempts?', Twitter, 28/V/2021.

[28] Council of the EU (2021), 'Outcome of Proceedings: Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade - Council conclusions approved by the Council at its meeting on 22 March 2021', 7290/21, 23/III/2021, p. 12.

[29] CERT-FR (2021), 'Campagne d'attaque du mode opératoire APT31 ciblant la France', cert.ssi.gouv.fr, 21/VII/2021.

[30] See the database here.

Eyes attribution that Hafnium is linked to the MSS–.[31] Meanwhile, the Romanian Ministry of Foreign Affairs also acknowledged the HR's Declaration and the NATO statement, and additionally expressed solidarity with the US and UK, while noting that APT40 is affiliated with the People's Republic of China –echoing to a degree the Five Eyes attribution that APT40 is the Ministry of State Security–.[32] Estonia and Romania are the only two EU member states that expressed some support for parts of the Five Eyes attribution, while the Romanian and Latvian Ministries of Foreign Affairs are the only ones to publish a written statement on their respective websites.[33] Three EU member states (Bulgaria, Italy and Spain) entirely ignored the HR's Declaration and instead opted to only tweet/retweet the NATO statement.

When it comes to the seven European non-EU NATO member states, only North Macedonia's Foreign Minister Bujar Osmani publicly supported the HR's Declaration.[34] Surprisingly, the UK kept its distance. Neither the Twitter account of the UK FCDO, the UK Mission to the EU nor UK Foreign Secretary Dominic Raab (re-)tweeted the HR's Declaration. The only UK recognition of the Declaration is found in the UK's public attribution statement under 'Notes to the editors', pointing out that 'the European Union has also made an announcement today'.[35]

Of the other Five Eyes member states, only the US State Department's Office of the Coordinator for Cyber Issues (CCI) retweeted the HR's Declaration. The CCI's behaviour on Twitter is of particular significance as it has been actively retweeting almost all the statements that other governments have made during this and many of the US coordinated public attribution campaigns in the past.[36] The CCI's actions might indicate the relevance of Twitter diplomacy and could even point to the US State Department analysing and keeping track of government statements on Twitter for political and impact-metric purposes.

The White House attribution statement merely mentions the 'European Union', while the statement of the Secretary of State, Antony Blinken, simply broadly talks about 'partners

[31] Estonian MFA (2021), 'Estonia expresses strong support for today's statements by the EU, US, UK & other allies which hold #China's Ministry of State Security responsible for Microsoft Exchange Server cyber operation & other incidents. #Estonia calls on China to act responsibly in cyberspace', Twitter, 19/VII/2021.

[32] Ministerul Afacerilor Externe (2021), 'Ministerul Afacerilor Externe se alătură demersurilor internaționale de condamnare a operațiunilor cibernetice maligne asupra Microsoft Exchange Server și a campaniei cibernetice a Grupării APT40', mae.ro, 19/VII/2021.

[33] Ministerial Afacerilor Externe (2021), 'Ministerul Afacerilor Externe se alătură demersurilor internaționale de condamnare a operațiunilor cibernetice maligne asupra Microsoft Exchange Server și a campaniei cibernetice a Grupării APT40', mae.ro, 19/VII/2021; Ministry of Foreign Affairs – Republic of Latvia (2021), 'Latvia raises its concern about irresponsible behavior in cyberspace', mfa.gov.lv, 19/VII/2021.

[34] Bujar Osmani (2021), 'Fully agree & support #EU & #NATO statements, denouncing malicious cyber activities, undertaken in contradiction w/ the norms of responsible state behaviour. We are determined to enhance coop. w/ our allies to improve the overall global security', Twitter, 19/VII/2021.

[35] UK FCDO (2021), 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', gov.uk, 19/VII/2021.

[36] The CCI likely only retweets government statements that it can find or that show up in its feed through the accounts it follows. This means that it is unclear whether the retweeting effort is a dedicated and organised task or whether it is unstructured and solely guided by the CCI communication's team.

and allies'.[37] Meanwhile, the Australian attribution statement only refers to 'international partners', Canada's attribution statement merely mentions 'allies' and New Zealand's GCSB Minister Andrew Little solely noted that 'New Zealand joins international condemnation'.[38]

Interestingly enough, the Chinese Foreign Ministry's spokesperson, Zhao Lijian, also failed to acknowledge the existence of the HR's Declaration in his regular press conference on 20 July 2021.[39] Instead, he only commented on the US and allied accusations. And, when asked, he briefly touched upon NATO without mentioning the latter's statement.

(3) NATO

The North Atlantic Council (NAC) –ie, the leading political decision-making body within NATO– published its statement on 19 July 2021, expressing its 'solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise'.[40]

Timeline-wise it is unclear when exactly the NATO member states started to deliberate on the NAC statement. It is highly likely that it was an item during the preparations for the NATO Brussels Summit on 14 June 2021, within the context of writing up the Summit's Communique. Notably, paragraph 55 of the Communique states that 'we call on China to uphold its international commitments and to act responsibly in the international system, including in the space, cyber, and maritime domains, in keeping with its role as a major power'.[41] Overall, however, the Communique mentioned China a mere 10 times –in contrast to Russia's 63 times–, which indicates NATO's heavy focus on Russia and an only slowly emerging consensus on China.

Within the cyber context, the NAC has expressed solidary at least three times before. On SolarWinds it stood in 'solidarity with the United States, following its 15 April announcement of actions to respond to Russia's destabilising activities'.[42] On the GRU's failed close hacking operation against the OPCW in 2018, the NATO allies stood in 'solidarity with the decision by the Dutch and British governments to call out Russia on

[37] The White House (2021), 'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China', Briefing Room, 19/VII/2021; Antony J. Blinken (2021), 'Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace', US Department of State, 19/VII/2021.

[38] Senator the Hon. Marise Payne, "Australia joins international partners in attribution of malicious cyber activity to China," foreignminister.gov.au, 19/VII/2021; Global Affairs Canada, 'Statement on China's cyber campaigns', canada.ca, 19/VII/2021; Tess McClure, 'New Zealand and China clash after west condemns 'malicious' cyber activity', The Guardian, 20/VII/2021.

[39] Embassy of the People's Republic of China in the United States of America (2021), 'Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on 20/VII/2021', china-embassy.org, 20/VII/2021.

[40] NATO (2021), 'Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise', nato.int, 19/VII/2021.

[41] NATO (2021), 'Brussels Summit Communiqué', nato.int, 14/VI/2021.

[42] NATO (2021), 'North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia', nato.int, 15/IV/2021.

its blatant attempts to undermine international law and institutions'.[43] And during the coronavirus pandemic, the NAC stood in 'solidarity with those who have been affected by malicious cyber activities and remain ready to assist Allies, including by continuing to share information, as they respond to cyber incidents that affect essential services'.[44]

Despite assertions by David Sanger in the *New York Times*' *The Daily* podcast that the 19 July statement marked the first time that NATO had condemned malicious cyber activities, the alliance had already done so a year earlier.[45] The NAC statement of 3 June 2020 literally says that 'we condemn destabilising and malicious cyber activities directed against those whose work is critical to the response against the pandemic, including healthcare services, hospitals and research institutes'.[46] The *New York Times* is also incorrect in asserting that the 19 July statement was 'the first such statement from NATO publicly targeting Beijing for cybercrimes'.[47] Nowhere in the NAC statement is crime referred to, in stark contrast to the White House's statement that explicitly condemns 'the PRC's use of criminal contract hackers to conduct unsanctioned cyber operations globally'.[48]

Other outlets including the *Washington Post*, *Forbes*, the *CNN* and many others, also wrongly asserted in some way, shape or form that the statement was 'the first time NATO has condemned Chinese cyber activities'.[49] The NAC statement does no such thing. It only acknowledges the national attribution statements made by the US, the UK and Canada, and condemned malicious cyber activities in purely general terms. It explicitly calls upon 'all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace'.[50] Thus, in contrast to the NATO statement on the OPCW hack, which explicitly stated that 'Russia must stop its reckless pattern of behaviour…', the NAC's 19 July statement is inherently weak, passive and non-confrontative.[51] It even goes so far as to express NATO's 'willingness to maintain a constructive dialogue with China based on our

[43] NATO (2018), 'Statement by NATO Secretary General Jens Stoltenberg on Russian cyber attacks', nato.int, 4/X/2018.

[44] NATO (2020), 'Statement by the North Atlantic Council concerning malicious cyber activities', nato.int, 3/VI/2020.

[45] The Daily (2021), 'Reacting to Chinese Cyberattacks', open.spotify.com, 21/VII/2021, timestamp: 6:19-6:40.

[46] NATO (2020), 'Statement by the North Atlantic Council concerning malicious cyber activities', nato.int, 3/VI/2020.

[47] Zolan Kanno-Youngs & David E. Sanger (2021), 'US Accuses China of Hacking Microsoft', nytimes.com, 19/VII/2021.

[48] The White House (2021), 'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China,' Briefing Room, 19/VII/2021.

[49] John Hudson & Ellen Nakashima (2021), 'US, allies accuse China of hacking Microsoft and condoning other cyberattacks', Washington Post, 19/VII/2021; Robert Hart (2021), 'US, NATO And Allies Accuse China Of Hacking Microsoft', Forbes, 19/VII/2021; Kevin Liptak (2021), 'US blames China for hacks, opening new front in cyber offensive', CNN, 20/VII/2021.

[50] NATO (2021), 'Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise', nato.int, 19/VII/2021.

[51] NATO (2018), 'Statement by NATO Secretary General Jens Stoltenberg on Russian cyber attacks', nato.int, 4/X/2018.

interests, on areas of relevance to the Alliance such as cyber threats, and on common challenges'.[52]

One interesting question that is currently still somewhat unresolved, is whether and how NATO might theoretically put forward a collective public attribution statement. The most straightforward option would be either via a consultation under Article 4 of the North Atlantic Treaty, or an invocation of Article 5 to trigger collective defence. Outside these two treaty mechanisms, a statement by the NAC could potentially include a collective attribution statement if all the 30 allied governments were to concur. Yet the political conundrum NATO will –and probably already has– very likely run into, is the same hurdle that prevents the 27 EU member states from agreeing to a collective public attribution. Furthermore, the question as to what a defensive military alliance like NATO might practically achieve from putting out a collective public attribution assessment during peacetime is difficult to answer. If the notion is to simply 'strengthen norms', then there are certainly other multinational non-military institutions that are better positioned to advance this goal diplomatically. If, however, the goal is to draw a red line in the sand whose violation could legally trigger offensive cyber operations by individual NATO member states, then perhaps NATO's first-ever collective public attribution call would be worth the political effort.

The tweets and retweets made by the official government Twitter accounts of the individual NATO member states (Ministries of Foreign Affairs, Ministries of Defence and the Permanent Representations and Missions to NATO) offer some statistically interesting data.[53] Among the 21 EU member states that are also NATO members, 10 remained silent on the NATO statement, nine posted a tweet in support and two simply retweeted NATO General Secretary Jens Stoltenberg's tweet (Bulgaria and Spain). Of the seven other European NATO member states, four posted a tweet in support (Albania, Iceland, North Macedonia and the UK), two merely retweeted Stoltenberg's tweet (Montenegro and Norway) and one remained completely silent (Turkey).

The UK NATO Delegation's Twitter account is somewhat curious. It posted tweets in support of the NAC statement, the UK FCDO attribution statement and retweeted NATO Secretary General Stoltenberg's tweet. But it was also the only official British government Twitter account that retweeted the HR declaration, the Canadian attribution statement and the statement of the US Secretary of State. It is unclear why the UK Delegation to NATO decided to retweet those specific statements and not any others. It could well be that this was a short-lived attempt to emulate the tracking efforts as conducted by the US State Department's CCI account.

The Norwegian government stands apart for one notable reason. It published a press release on 19 July 2021 that connects the data breach of the Norwegian parliament in March 2021 to the Microsoft Exchange campaign. In the press release, the Norwegian government assessed –based on a thorough intelligence review– that the activity was

[52] NATO (2021), 'Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise', nato.int, 19/VII/2021.

[53] See the database here.

carried out 'from China' and noted that several allies, the EU and Microsoft confirm this.[54] As a reaction, the Norwegian Foreign Ministry summoned the Chinese Ambassador, while the Chinese Embassy in Norway sent out statements to various news outlets noting that it was waiting for the Norwegian side to provide evidence and facts to prove the claim and that it was strongly opposed to baseless allegations.[55]

Going a step further and comparing the public support of the 27 NATO member states for the NATO statement (excluding Canada, the UK and the US) with the public support of the 27 EU member states for the HR's Declaration, the result is that 18 EU member states supported the HR's Declaration (66%) and 16 NATO member states supported the NATO statement (59%). Among the 21 countries that are both NATO and EU members the results were: 14 in support of the HR's declaration (66%) and 11 in support of the NATO statement (52%). A mere eight countries publicly supported both statements (38%). Looking at the six European non-EU NATO members (excluding the UK) the numbers clearly favoured one side: only one supported the HR's declaration (16%), while five supported the NATO statement (83%). Only one country publicly supported both statements (16%). Among the six EU member states that are not NATO members, the numbers clearly favoured the other: four supported the HR's declaration (66%), while none supported the NATO statement (0%). The conclusion from the numbers is that member states seem to politically pick and choose which statement to publicly support. This stands in contrast to the broader expectations of like-minded countries throwing their public support behind all political statements on normative behaviour and the applicability of international law in cyberspace.

Whether the behaviour of government Twitter accounts matters or not is still up for debate. Some might rightfully argue that political support for the NATO statement or the HR's Declaration is already implied when the individual member states agreed or not disagreed to drawing up and publishing the statements in the first place. Following that reasoning, Twitter posts and retweets are just the public relations component in addition to already finalised political agreements. Similarly, some governments might be more active on Twitter than others or have different political priorities and issue sensitivities at the time. On the other side of the argument are the voices that view Twitter posts and retweets of official government accounts as a specific form of public support for the statements involved, as well as an opportunity to clarify or even go beyond the common denominator as agreed on within the NAC and the European Council.

Finally, among the Five Eyes, the UK, the US and Canada do reference 'allies' in their public attribution statements, but only the White House explicitly mentions NATO.[56]

[54] Regjeringen.no (2021), 'Datainnbruddet i Stortingets e-postsystem', regjeringen.no, 19/VII/2021.

[55] Andreas Løf & Fredrik Moen Gabrielsen (2021), 'Kina etterlyser bevis for at de sto bak IT-angrepet mot Stortinget', Aftenposten, 19/VII/2021.

[56] UK FCDO (2021), 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', gov.uk, 19/VII/2021; The White House (2021), 'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China', Briefing Room, 19/VII/2021; Global Affairs Canada (2021), 'Statement on China's cyber campaigns', canada.ca, 19/VII/2021.

(4) Five Eyes

Among the Five Eyes member states (Australia, Canada, New Zealand, the UK and the US), the White House's public attribution statement is clearly the longest, at 1,579 words.[57] In fact, it was longer than the combined statements of the UK's FCDO (576 words), New Zealand's GCSB (261 words), the Australian government (349 words) and the Canadian government (346 words).[58] If that were not enough, the US Secretary of State also issued his own separate statement (336 words).[59]

The one and only common thread that binds together all five government attribution statements is that they mention the targeting of Microsoft Exchange Server. The UK and New Zealand attribute the campaign to 'Chinese state-sponsored actors'. The Australian and Canadian governments point explicitly at the Chinese MSS, while the White House attributes it with a high degree of confidence to malicious cyber actors affiliated with the Chinese MSS.

The attribution differences are very likely caused by different intelligence insights and national threat landscape visibilities, and a divergence in opinion on what the adversarial Chinese campaign was actually all about. It seems likely that the Australian and Canadian governments defined the campaign as only encompassing the initial exploitation by Hafnium, meaning that for them the latter was simply the MSS. By contrast, the UK and New Zealand talked about several 'Chinese state-sponsored actors', meaning their definition likely stretched from the initial Hafnium compromise to the follow-up operations by other Chinese threat actors –including Tick, Calypso and Winnti, as reported by ESET–. [60] Meanwhile, the White House probably ran into significant difficulties discerning what exactly Hafnium was and how the group or persons were interfacing with the MSS. The non-use of the word Hafnium in the White House statement, and the absence of indictments and criminal charges against the Chinese individuals responsible for the MS Exchange campaign, were highly likely indicative of current US uncertainties. Notably, the UK is the only government that specifically referenced Hafnium in its statement.

When it comes to APT31, four of the Five Eyes governments did not reference it at all in their statements. The UK FCDO attributed the MSS with being 'behind activity known by

[57] The White House (2021), 'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China', Briefing Room, 19/VII/2021.

[58] UK FCDO (2021), 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', gov.uk, 19/VII/2021; Hon. Andrew Little (2021), 'New Zealand condemns malicious cyber activity by Chinese state-sponsored actors', beehive.govt.nz, 19/VII/2021; Senator the Hon. Marise Payne (2021), 'Australia joins international partners in attribution of malicious cyber activity to China', foreignminister.gov.au, 19/VII/2021; Global Affairs Canada (2021), 'Statement on China's cyber campaigns', canada.ca, 19/VII/2021.

[59] Antony J. Blinken (2021), 'Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace', US Department of State, 19/VII/2021.

[60] Matthieu Faou *et al*. (2021), 'Exchange servers under siege from at least 10 APT groups', ESET, 10/III/2021.

cyber security experts as… "APT31"'.[61] And the UK NCSC assessed that 'APT 31 is a group of contractors working directly for the Chinese Ministry of State Security' and specifically noted that APT31 targeted the Finnish Parliament in 2020.[62] Tellingly, the absence of any APT31 references in the other Five Eyes statements stands in stark contrast to the importance that the EU and its member states attach to the mentioning of APT31 in the HR's Declaration.

Curiously, while all the Five Eyes name the Chinese Ministry of State Security in their statements, only Canada, the UK and New Zealand connected the MSS to APT40. The Australian statement is devoid of any APT40 references. And neither the White House nor the State Department's statements mention APT40 either. It is also curious to note that of all the Five Eyes statements, only the UK's and Canada's specifically included a reference to Hainan. The Canadian government noted that 'APT 40 almost certainly consists of elements of the Hainan State Security Department's regional MSS office', while the UK NCSC judged that 'APT40 is highly likely sponsored by the regional MSS security office, the MSS Hainan State Security Department (HSSD)'.[63] The attribution difference between 'elements of' and 'sponsored by' are significant enough to open up the question as to whether APT40 is a state or non-state actor and to what degree.

New Zealand's statement stands out for several reasons. First, the Government Communications Security Bureau (GCSB) is the only intelligence agency among the Five Eyes members that does not have an official Twitter account. Therefore, while the public attribution statement made by GCSB Minister Andrew Little was published on the official website of the New Zealand government and his comments were covered in various New Zealand and British media outlets, neither the official Twitter accounts of the GCSB Minister, New Zealand's Foreign Minister nor New Zealand's Ministry of Foreign Affairs & Trade bothered to tweet the GCSB statement.[64] In fact, among the Five Eyes statements, New Zealand is the only government whose Foreign Ministry remained completely silent on the matter. Despite this lack of communication and assertion by the New Zealand government, some analysts have nonetheless argued that 'the harsh statement on China issued by New Zealand on Monday is a realist shot across the bow'.[65] While this might be the perception in New Zealand, from an outside perspective the 19 July statement is both in tone and substance very similar to the GCSB attribution statement made on 21 December 2018, when it called out the MSS on APT10.[66] The only major difference this time is that the statement was only published on the New

[61] UK FCDO (2021), 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', gov.uk, 19/VII/2021.

[62] Ibid.

[63] Ibid.

[64] Hon. Andrew Little (2021), 'New Zealand condemns malicious cyber activity by Chinese state-sponsored actors', beehive.govt.nz, 19/VII/2021.

[65] Geoffrey Miller (2021), 'New Zealand's Statement on China's Cyberattacks: A Shot Across the Bow', The Diplomat, 22/VII/2021.

[66] Government Communications Security Bureau (2018), 'Cyber campaign attributed to China', gcsb.govt.nz, 21/XII/2018.

Zealand government website, while the 2018 statement was published on both the GCSB and NCSC websites.[67]

Canada's approach towards public attribution statements applies a different logic. Back in 2018, the Communications Security Establishment (CSE) –which is Canada's sister agency to the NSA– was responsible for publishing its official attribution statements. Around October 2020 that practice changed, when the sole responsibility moved from CSE to Global Affairs Canada (ie, the Canadian Department for Foreign Affairs, Trade, and Development).[68] As a result, while the 2018 CSE statement on APT10 merely noted that it was assembled through a joint effort between CSE, 'its Canadian Centre for Cyber Security (Cyber Centre), and other departments and agencies', the 19 July 2021 statement was issued in the name of three Canadian Ministers: Foreign Affairs, National Defence, and Public Safety and Emergency Preparedness.[69] This upgrade in substantial political backing was first apparent on 15 April 2021, when the three Ministers issued Canada's public attribution statement on the SolarWinds campaign.[70]

Australia has similarly upgraded the political backing for its public attribution statements. Back in December 2018, when Australia attributed APT10 to the MSS, only two Ministers signed the attribution statement: Foreign Affairs (Marise Payne) and Home Affairs (Peter Dutton).[71] Following a cabinet reshuffle in March 2021, Peter Dutton was appointed Minister for Defence and Karen Andrews assumed the office of Minister for Home Affairs. This change also brought about an upgrade in political backing, as the government's SolarWinds attribution to Russia in April 2021 was carried out by three Ministers: Foreign Affairs (Marise Payne), Home Affairs (Karen Andrews) and Defence (Peter Dutton).[72] The same political dynamic played out on 19 July 2021.[73] In terms of government Twitter activity, all three Australian and all three Canadian Ministers tweeted about their respective public attribution statements. This is in stark contrast to the British (only the Foreign Office), New Zealand (only GCSB) and the US attributions (only White House and State Department).

When it comes to US statements, it should be recalled that back in December 2018, then Secretary of State Pompeo and then Secretary of Homeland Security Nielsen put out a joint attribution statement on 'Chinese cyber actors associated with the Chinese Ministry

[67] Hon. Andrew Little (2021), 'New Zealand condemns malicious cyber activity by Chinese state-sponsored actors', beehive.govt.nz, 19/VII/2021; Government Communications Security Bureau (2018), 'Cyber campaign attributed to China', gcsb.govt.nz, 21/XII/2018; National Cyber Security Centre (2018), 'Cyber campaign attributed to China', ncsc.govt.nz, 21/XII/2018.

[68] Global Affairs Canada (2020), 'Canada expresses concern over pattern of malicious cyber activity by Russian Military Intelligence', canada.ca, 19/X/2020.

[69] Communications Security Establishment (2018), 'Canada and Allies Identify China as Responsible for Cyber-Compromise', cse-cst.gc.ca, 20/XII/2018.

[70] Global Affairs Canada (2021), 'Statement on SolarWinds Cyber Compromise', canada.ca, 15/IV/2021.

[71] Senator the Hon Marise Payne (2018), 'Attribution of Chinese cyber-enabled commercial intellectual property theft', foreignminister.gov.au, 21/XII/2018.

[72] Senator the Hon. Marise Payne (2021), 'Attribution of cyber incident to Russia', foreignminister.gov.au, 15/IV/2021.

[73] Senator the Hon. Marise Payne (2021), 'Australia joins international partners in attribution of malicious cyber activity to China', foreignminister.gov.au, 19/VII/2021.

of State Security'.[74] This was the first and to date only time that a Secretary of Homeland Security put out a written attribution statement. The US Department of Defense was also visibly involved back in December 2018, with the Director of the DoD's Defense Criminal Investigative Service speaking at the DoJ's press conference announcing the criminal charges against two APT10 members.[75] Notably, the White House did not publish a written attribution statement on that occasion.

Similar to the 19 July White House statement, the 2018 joint statement attributed activities to the MSS without using the industry designations for the threat actors in question. This is not usually a problem because government attribution statements generally only focus on one adversarial campaign or one specific threat actor. The White House statement of 19 July creates a bit of a problem in that respect, as it tries to knit one grand narrative that is supposedly backed by all of its allies and partners. The White House narrative consists of three different attribution parts in the following order: (a) the general observation of the 'PRC's use of criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit'; (b) the DoJ 'announcing criminal charges against four MSS hackers' (ie, APT40); and (c) 'MSS-affiliated cyber operators exploiting 0-day vulnerabilities in MS Exchange Server' (ie, Hafnium).

On item (a) no ally or partner except for Australia expressed serious concern that the MSS is 'engaging contract hackers who have carried out cyber-enabled intellectual property theft for personal gain'.[76] The absence of widespread support on this item is irritating, since it is the very first item the White House statement mentions after gloating about the 'unprecedented group of allies and partner' that are 'joining the United States in exposing and criticizing the PRC's malicious cyber activities'.[77] If, as a senior administration official told the *New York Times*, 'the Biden administration settled on corralling enough allies to join the public denunciation of China to maximize pressure on Beijing to curtail the cyberattacks', then why was the US unable to garner wide-spread support on their number one item that –according to the White House itself– has been occurring since at least October 2018?[78]

The Chinese contract hacker's usage of ransomware and cyber-enabled extortion in their side-campaigns should have particularly resonated to some extent with European normative and cybercriminal concerns, even though the specific Chinese campaigns might not have yet occurred in Europe itself. The silence of all EU members on this item

[74] Michael R. Pompeo & Kirstjen M. Nielsen (2018), 'Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen M. Nielsen', US Department of Homeland Security, 20/XII/2018.

[75] US Department of Justice (2018), 'Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information', Office of Public Affairs, 20/XII/2018.

[76] Senator the Hon. Marise Payne, 'Australia joins international partners in attribution of malicious cyber activity to China', foreignminister.gov.au, 19/VII/2021.

[77] The White House (2021), 'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China', Briefing Room, 19/VII/2021.

[78] Zolan Kanno-Youngs & David E. Sanger (2021), 'US Accuses China of Hacking Microsoft', nytimes.com, 19/VII/2021.

should give the White House pause for thought and make the State Department rethink whether the US's allies and partners are actually like-minded and truly aligned with Washington's concerns in cyberspace.

On Item (b) the US Grand Jury indictment of the four MSS operatives describes activities between 2011 and 2018. This suggests that it is not the most recent and pressing case that would have warranted a coordinated public attribution campaign. Similarly, of the 22 companies and facilities that the defendants breached according to the indictment, 15 were located in the US, three in Malaysia, two in Saudi Arabia, one in Cambodia, one in Switzerland and one in Germany.[79] Given the absence of high-volume and high-profile APT40 activity in Europe, it should come as no surprise that the majority of NATO and EU member states were rather timid in this respect. Among the Five Eyes members, only Canada specifically noted that APT40 'targeted critical research in Canada's defence, ocean technologies and biopharmaceutical sectors in separate malicious cyber campaigns in 2017 and 2018'.[80] In contrast, Australia's statement did not mention APT40 even once. New Zealand merely referred to links between APT40 and malicious cyber activity in the country,[81] and the UK talked broadly about APT40 'targeting maritime industries and naval defence contractors in the US and Europe'.[82] Meanwhile, the government of Japan explicitly stated that 'Japanese companies were also targeted in the aforementioned case by the group known as APT40'.[83]

Item (c) was the newest and most important item for the coordination among allies and partners on calling out China's malicious activities. In most –if not all– allied and partner territories, numerous system and networks were highly likely affected by Hafnium's indiscriminate exploitation of MS Exchange Server 0-day vulnerabilities and/or the follow-up campaigns by Tick, Calypso, Winnti and other groups. Unsurprisingly, the attribution statements of all the Five Eyes members mention the MS Exchange Server campaign. The HR's Declaration mentions it, and so does NATO. And yet it is the last and content-wise shortest attribution item in the White House statement.

The absence of any DoJ charges and Treasury sanctions in connection with the MS Exchange campaign likely suggests a current lack of US intelligence insights into Hafnium. This could be due to Hafnium being a fairly new threat actor, which would line up with Microsoft publicly discussing Hafnium activity for the first time on 2 March 2021.[84] Or it could indicate that the US intelligence community ran into significant difficulties gathering intelligence on the group and identifying individual Hafnium members. Thus, it was not a realistic option for the White House to wait another month or two so the DoJ

[79] United States District Court, Southern District of California (2021), 'United States of America v. Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin, and Wu Shurong, November 2019 Grand Jury, filed on 28/V/2021.

[80] Global Affairs Canada (2021), 'Statement on China's cyber campaigns', canada.ca, 19/VII/2021.

[81] Hon. Andrew Little (2021), 'New Zealand condemns malicious cyber activity by Chinese state-sponsored actors', beehive.govt.nz, 19/VII/2021.

[82] UK FCDO (2021), 'UK and allies hold Chinese state responsible for a pervasive pattern of hacking', gov.uk, 19/VII/2021.

[83] Yoshida Tomoyuki (2021), 'Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind', Ministry of Foreign Affairs of Japan, 19/VII/2021.

[84] Tom Burt (2021), 'New nation-state cyberattacks', Microsoft, 2/III/2021.

might potentially have enough intel to push out indictments on Hafnium. In turn, this likely also means that the White House will be unable to rally support around the MS Exchange campaign again when the DoJ indicts individual Hafnium members. As of the time of writing it is still unknown why the White House deemed it necessary to throw the MS Exchange campaign into its attribution mix. A focus on APT40 and APT31 would have been entirely sufficient to rally support on calling out Chinese espionage campaigns, highlight the MSS's use of hackers-for-hire and the MSS turning a blind eye on their contractors running cybercriminal campaigns on the side.

(5) Japan

The Japanese government's written attribution statement on 19 July 2021 was delivered by the press secretary of the Ministry of Foreign Affairs (MOFA).[85] This was only the second time the Japanese government joined a coordinated public attribution campaign. The other occasion was in December 2018 on APT10, whose written statement was also delivered by MOFA's press secretary.[86] It is unknown why these statements are not delivered by the Japanese Foreign Minister, but a partial explanation could be Tokyo's desire to preserve ministerial level talks with China on other bi- and multilateral issues. As such, the non-reaction to the Japanese statement by the Chinese Foreign Ministry could be interpreted as political reciprocity and recognition for non-escalation.

Importantly, the MOFA statement back in 2018 merely acknowledged the Five Eyes attribution that APT10 is based in China but did not put forward Japan's own attribution assessment. The 19 July statement is very different in this regard. For the first time ever 'Japan also assesses that it is highly likely that the Chinese government is behind APT40'. On top of this attribution assessment, the Japanese government also highlighted the attribution call made by Japanese law enforcement back in April 2021 that Tick is 'Unit 61419 of the Chinese People's Liberation Army'.[87]

The Japanese attribution call on Tick goes back to a law enforcement investigation into an adversarial campaign that breached Japan's Aerospace Exploration Agency (JAXA) and 200 other Japanese companies between 2016 and 2020. The Tokyo Metropolitan Police interrogated two people of interest who have since left Japan:[88] a 30-year-old male Chinese citizen who works as a systems engineer for an unnamed Chinese IT company, and a Chinese overseas student who was likely enrolled in a Japanese university.[89] The Chinese engineer admitted during his interrogation that he 'sought to make pocket money' by forging documents to be able to rent multiple servers in Japan, and then sell the account credentials to the highest bidder on likely Chinese underground

[85] Yoshida Tomoyuki (2021), 'Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind', Ministry of Foreign Affairs of Japan, 19/VII/2021.

[86] Takeshi Osuga (2018), 'Cyberattacks by a group based in China known as APT10', Ministry of Foreign Affairs of Japan, 21/XII/2018.

[87] Catalin Cimpanu (2021), 'Japanese police say Tick APT is linked to Chinese military', The Record, 20/IV/2021.

[88] The Japan Times (2021), 'Chinese military seen behind Japan cyberattacks', 20/IV/2021.

[89] Yomiuri (2021), 'ＪＡＸＡにサイバー攻撃か、中国共産党員の男を書類送検…関与人物の特定は異例', 20/IV/2021.

forums.[90] Japanese law enforcement believes that PLA Unit 61419 purchased these credentials and then used the Japanese-based servers as kick-off points for the Tick campaign against JAXA and other Japanese companies.[91] According to Mainichi there does not seem to be any direct connection between the Chinese engineer and the PLA.[92]

The second suspect –the Chinese student– admitted during his interrogation that he was introduced by an acquaintance (mediator) to a woman in China (handler). Yomiuri and NHK reported that the woman's husband was a member of PLA Unit 61419.[93] Tokyo Metropolitan Police searched the student's mobile phone and emails to reconstruct his communications with said female handler. The student was in fact pressured and received specific instructions to 'contribute to the nation'. His tasks included fraudulently renting a server in Japan, purchasing Japanese security software and buying a specific secure USB stick made in Japan.[94] According to Mainichi the Metropolitan Police believes that that the PLA was trying to study the vulnerability of Japanese security software.[95] And according to Yomiuri the USB stick was for researching and analysing the safety measures of specific Japanese products.[96] Yomiuri also reports that according to Japanese law enforcement, Tick and PLA Unit 61419 'seem to be almost the same'.[97] As of the time of writing it unclear whether the two suspects have been charged nor whether the Japanese government has requested their extradition.

The law enforcement attribution of Tick being PLA Unit 61419 does not really come as a surprise given that 'the Japanese National Police Agency is currently the most capable [Japanese] intelligence agency – focusing primarily on combating cybercrime, cyber terrorism, and cyber espionage'.[98] That being said, the 19 July attribution call by the Japanese government on APT40 is still somewhat of a mystery. It is currently unknown which Japanese government agency made the attribution call and why that agency was unable –or unwilling– to publicly connect APT40 to the MSS. The only part we do know for certain is that on 19 July, the National Police Agency (NPA) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) released a written statement in support of the MOFA statement, that confirmed that APT40 was targeting Japanese companies.[99]

[90] Mainichi (2021), '人民解放軍がサイバー攻撃関与か　中国人書類送検　JAXA 標的', 20/IV/2021.

[91] The Asahi Shimbun (2021), 'Police: Chinese men involved in cyberattacks against JAXA', 20/IV/2021.

[92] Mainichi (2021), '人民解放軍がサイバー攻撃関与か　中国人書類送検　JAXA 標的', 20/IV/2021.

[93] Yomiuri (2021), '「国に貢献しなさい」中国軍人の妻が元留学生に指示か…ＪＡＸＡサイバー攻撃事件', 21/IV/2021; NHK (2021), 'サイバー攻撃 中国共産党員の男ら警視庁事情聴取も その後出国', 20/IV/2021.

[94] Ibid.

[95] Mainichi (2021), '中国ハッカー集団、JAXA など 200 機関にサイバー攻撃疑い　軍関与か', 20/IV/2021.

[96] Yomiuri (2021), '「国に貢献しなさい」中国軍人の妻が元留学生に指示か…ＪＡＸＡサイバー攻撃事件', 21/IV/2021.

[97] Yomiuri (2021), 'ハッカー集団　中国軍と一体か', 21/IV/2021.

[98] Stefan Soesanto (2021), 'Outward Defense - Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time', Konrad Adenauer Stiftung, Facts & Findings, nr 449, June.

[99] NISC & NPA (2021), '中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起）', nisc.go.jp, 19/VII/2021.

Japan's 19 July attribution statement also stands out on another item: it does not mention the MS Exchange campaign at all. Therefore, the one red thread that connects all other statements on that day is not echoed by the Japanese government. The most plausible explanation for this oddity is that the MS Exchange Server is simply not widely used in Japan. According to a blog post published by Yutaka Sejiyama at Macnica Networks on 7 March 2021 the amount of Exchange Servers in Japan vulnerable to Proxylogon stood at a mere 194 compared with 167,055 globally.[100]

The Japanese non-focus on the MS Exchange campaign might also explain why the White House statement ranked the MS Exchange campaign last in its attribution call, and it would explain why the HR's Declaration mentions APT40 out of the blue. Putting these three things together it is highly likely that Washington used the time and context of Hafnium's MS Exchange campaign to approach its allies and partners on calling out China, but politically pushed for the inclusion of APT40 to underpin the one area where it had substantial evidence and intelligence at hand. Therefore, for Washington, 19 July was never really about Hafnium and the MS Exchange campaign, but first and foremost about APT40 and the DoJ's criminal charges. If this is true, then for some as yet unknown reason, Washington's strategy failed to achieve the inclusion of APT40 in the NAC statement.

(6) Conclusion

Given the absence of a clear red thread that runs through the statements made by the Five Eyes, the EU, NATO and Japan, one has to sincerely question the supposed like-mindedness of the governments involved, as well as their ability to forge a coherent message toward Beijing's behaviour in cyberspace. A mere two out of 27 EU member states chose to publish their own written statements, while the other 25 were either only willing to publicly supporting the HR's Declaration on Twitter or entirely ignored it. Some analysts will certainly argue that these numbers show EU unity, when, in fact, they show an act of abdication: an abdication of individual member state responsibility to go beyond the HR's Declaration. Instead, the overwhelming majority of EU member states chose to hide behind the weakest common denominator –the EU cyber diplomacy toolbox– to confront Beijing.

The same behavioural abdication is visible in the NAC statement. Rather than condemning Beijing's malicious conduct in cyberspace, demanding an immediate halt to its activities, and maybe even putting out the first ever coordinated NATO public attribution statement, the 30 allies were only willing to express their solidarity with those affected by the MS Exchange campaign.

By contrast, the Five Eyes members are the most coherent group when comes to attribution, calling out Beijing on the MS Exchange campaign, and highlighting APT40 activity. However, for one reason or another, the Five Eyes failed to achieve consensus

[100] Yutaka Sejiyama (2021), 'ProxyLogon のまとめと Exchange Server の利用状況について', blog.macnica.net, 8/III/2021.

on the point that Beijing is using ‘criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit’.

Meanwhile, the Japanese government statement was by far the biggest surprise. Not only did it re-echo the law enforcement assessment that Trick is PLA Unit 61419, but it also decided to put forward its own public attribution assessment on APT40. Time will tell whether in the not-so-distant future Japan’s Foreign Minister will release Tokyo’s attribution statements, and whether the Japanese Defence Minister and/or a high-ranking law enforcement official will join in to somewhat replicate the political backing as exercised by the Canadian and Australian governments.