EU declarations, DDoS attacks, and the erosion of norms and rules for State behaviour in cyberspace

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

Theme

The geopolitical shift caused by the Russian invasion of Ukraine has resulted in deliberate inconsistencies in EU Member States' applications of international law governing cyberspace and adherence to the United Nations cyber norms framework.

Summary

On 18 July 2022, the Belgian Ministry of Foreign Affairs (MFA) released a unilateral declaration – for the first time ever – that attributed the 2021 breaches of the Federal Public Service Interior (FPS interior) and the Ministry of Defence (MoD) to four different Chinese advanced persistent threat (APT) actors.[1] Twenty-four hours after the MFA's public announcement, the EU High Representative for Foreign Affairs and Security Policy published a declaration on behalf of the EU and its Member States in response to 'the latest distributed denial-of-service (DDoS) attacks against several EU Member States and partners claimed by pro-Russian hacker groups.'[2] The public release of two European declarations (a unilateral one and a collective one) so closely together and covering two very different types of cyber incidents (espionage vs hacktivism), threat actors (APT vs non-state actors) and countries (China vs Russia) is unusual and warrants a closer look..

Analysis

At the technical level, we know from several Belgian media outlets, the intrusion into the MoD's network took advantage of the Log4j vulnerability (known as Log4Shell). Alibaba Cloud Security researcher Chen Zhaojun responsibly disclosed Log4Shell to the Apache Software Foundation on 24 November 2021.[3] Two weeks later, on 9 December 2021, Log4Shell was disclosed to the public. However, by 1 December, Cloudflare had already detected limited probing of systems for the Log4Shell vulnerability throughout the world.[4] There are several plausible explanations that could account for this oddity. It could be

[1] Belgian MFA (2022) 'China: Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors', 18 July.

[2] EU Council (2022) 'Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine', 19 July.

[3] William Turton et al. (2021) 'Inside the Race to Fix a Potentially Disastrous Software Flaw', *Bloomberg*, 14 December.

[4] John Graham-Cumming (2021), 'Exploitation of Log4j CVE-2021-44228 before public disclosure and evolution of evasion and exfiltration', *Cloudflare Blog*, 14 December.

the case that multiple researchers found the Log4j vulnerability roughly around the same time (bug collision). It could also be the case that someone at Alibaba or Apache informed an outside party about the existence of Log4Shell. Or the conversation between Chen and Apache may not have been as secure as the two parties thought.

The Belgian MoD detected the intrusion into its network on Thursday 16 December 2021 and responded with a host of internal measures to isolate and contain the affected systems. On the Sunday night (19 December) the MoD publicly acknowledged that it had fallen victim to a severe cyberattack.[5] Speaking to VRT news the next day, MoD spokesperson Olivier Severin explained that 'all weekend our teams have been mobilized to control the problem, continue our activities, and warn our partners […]. The priority is to keep the network operational. We will continue to monitor the situation. [The MoD] will not provide any further information at this stage.'[6] Over the following weeks, the MoD essentially disconnected, rebuilt and purged its network. By mid-January 2022, Defence Minister Ludivine Dedonder stated that its 'network has indeed been cut off from the internet for a long time. That was necessary to be able to check whether everything was safe. Since Tuesday afternoon [11 January 2022], emails can be sent outside again.'[7] In June 2022, Minister Dedonder also ordered the removal of around 300 Huawei routers from the MoD network.[8] Lastly, the declaration by the Minister of Foreign Affairs on behalf of the Belgian Government on 18 July attributes the intrusion into the MoD network to the Chinese 'hacker groups known as UNC 2814/GALLIUM/SOFTCELL.'[9]

In 2018, US-headquartered cybersecurity company Cybereason identified an espionage campaign they named Operation Soft Cell. As Cybereason explains, 'based on the data available to us, Operation Soft Cell has been active since at least 2012, though some evidence suggests even earlier activity by the threat actor against telecommunications providers. […] We've concluded with a high level of certainty that the threat actor is affiliated with China and is likely state sponsored.'[10] Microsoft tracks the same threat actor under the designation Gallium. In December 2019, the Microsoft Threat Intelligence Center (MSTIC) published a comprehensive blog post stating it was 'raising awareness of the ongoing activity by a group we call GALLIUM, targeting telecommunication providers. […] This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed. […] GALLIUM domains have been observed

[5] Bart Haeck (2021) 'Defensie sinds donderdag slachtoffer van cyberaanval', *De Tijd*, 20 December.

[6] Jens Franssen (2021) 'Defensie slachtoffer van zware cyberaanval, deel netwerk al dagen plat', *VRT*, 20 December.

[7] Het Laatste Nieuws (2022) 'Cyberaanval tegen Defensie veel ernstiger dan eerst gedacht', *HLN*, 12 January.

[8] De Standaard (2022) 'Overheid dumpt Chinese routers uit vrees voor spionage', 20 July.

[9] Belgian MFA (2022) 'China: Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors', 18 July; see also https://twitter.com/iiyonite/status/1578394309136621571.

[10] Cybereason (2019) 'Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers', *MaliciousLife*, 25 June.

hosted on infrastructure in mainland China, Hong Kong SAR, and Taiwan.'[11] UNC is a designation used by US threat intelligence company Mandiant to classify uncategorised threat groups.[12] Sadly, as of this writing, Mandiant has not publicly released any information on UNC 2814. It is therefore unknown when Mandiant first detected UNC 2814 and in what context it did so. However, it is important to highlight that: (a) the EU never released a declaration in response to the exploitation of Log4j; and (b) the EU has so far not published a declaration that mentions UNC 2814, Gallium or Soft Cell.[13]

By contrast, the intrusions into the network of the FPS Interior were detected by pure accident. Back in March 2021, the FPS Interior tasked the Centre for Cyber Security Belgium (CCB) to secure its systems against the ProxyLogon vulnerability in Microsoft Exchange Server.[14] ProxyLogon was responsibly disclosed in early January by Orange Tsai, principle security researcher at Taiwan-based cybersecurity company Devcore.[15] US cybersecurity company Volexity and Denmark-based Dubex subsequently detected an APT actor leveraging ProxyLogon and two additional zero-day vulnerabilities in their campaigns.[16] On 2 March 2021, Microsoft published a blog post identifying the threat actor as Hafnium and concurrently released two urgent patches to fix the ProxyLogon vulnerabilities.[17] The CCB applied these patches to the FPS Interior systems and continued to monitor the network, subsequently discovering suspicious network activity. Further analysis revealed that one or more intruders gained access to the FPS Interior network as long ago as April 2019. The CCB explained that 'the perpetrators acted purposefully, which suggests espionage.'[18] According to Miguel De Bruycker, managing director of the CCB, 'there was no classified information on the network. The systems that process classified information were also not affected […]. So, it really concerns the internal documents of the FPS Interior, which may have been accessed by the adversary.'[19] The Federal Public Prosecutor's Office subsequently opened an investigation into the case, but at the time of writing no information has been publicly released explaining how the intruders gained access to the network. The declaration by the Belgian Minister of Foreign Affairs on 18 July attributes the FPS intrusion to three Chinese APT groups: APT 27, APT 30 and APT 31. At the time of writing, it is unknown whether all three groups were detected by the CCB in March 2021, or whether the declaration also refers to campaigns that were detected at a much earlier or even later point in time.

[11] Microsoft (2019) 'GALLIUM: Targeting global telecom', Microsoft Threat Intelligence Center, 12 December.

[12] Mandiant (n.d.) 'Uncategorized (UNC) Threat Groups'.

[13] Council of the European Union response to a Freedom of Information request, 4 October 2022.

[14] IBZ (2021) 'De FOD Binnenlandse Zaken heeft het hoofd geboden aan een cyberaanval en moderniseert zijn informatica-infrastructuur (25 mei 2021)', Federale Overheidsdienst Binnenlandse Zaken, 25 August.

[15] Orange.tw (2021) 'A New Attack Surface on MS Exchange Part 1 - ProxyLogon!', 6 August.

[16] Josh Grunzweig et al. (2021) 'Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities', *Volexity Blog*, 2 March;

[17] Microsoft (2021) 'HAFNIUM targeting Exchange Servers with 0-day exploits', MSTIC, 2 March.

[18] CCB (2021) 'De FOD Binnenlandse Zaken heft het hoofd geboden aan een cyberaanval', Centre for Cyber Security Belgium, n.d.

[19] Hanne Decre and Loutfi Belghmidi (2021) 'Twee jaar lang "doelbewuste" cyberaanval op overheidsdienst Binnenlandse Zaken: "Dit is spionage"', *VRT*, 25 May.

From a European perspective there are two points of reference. First, the EU did issue a declaration on 19 July 2021 – almost one year prior – that stated that 'the compromise and exploitation of the Microsoft Exchange server undermined the security and integrity of thousands of computers and networks worldwide, including in the Member States and EU institutions.'[20] The EU attributed this activity to 'Advanced Persistent Threat 40 [Hafnium] and Advanced Persistent Threat 31 [Zirconium].' APT 31 prominently entered the news cycle in Europe back in March 2021, when the Finnish Central Criminal Police (KRP) and the Finnish Security Intelligence (SUPO) attributed the autumn 2020 breach of the Finnish Parliament's internal IT systems to APT 31.[21] Three months later, in June 2021, Hanne Blomberg, Norway's Head of Counterintelligence, also publicly attributed the 2019 breach of the Norwegian software company VISMA to APT 31.[22]

Second, back in March 2021, Slovakia-based cybersecurity company ESET reported having identified at least ten APT groups exploiting ProxyLogon. Among them was LuckyMouse – Kaspersky's designation for APT 27. Furthermore, in January 2022, the German Federal Office for the Protection of the Constitution (BfV) published a report that warned German businesses that APT 27 had been actively exploiting flaws in the Zoho AdSelf Service Plus software (CVE-2021-40539) since at least March 2021.[23] The same vulnerability was later exploited to breach the servers of the International Committee of the Red Cross (ICRC) in November 2021, which likely led to the exfiltration of the personal data of more than 515,000 people.[24] At the time of writing, the breach of the ICRC has not been attributed to a specific threat actor.

In contrast, APT 30 (Naikon), also known as the Chinese People's Liberation Army Unit 78020, has historically focused almost exclusively on targets in South-East Asia.[25] For the unit to appear in a Belgian Government network is quite out of the ordinary. However, given that the Belgian Government has not published any of the collected underlying forensic evidence or elaborated on the confidence level of the attribution, it is impossible to properly examine, interpret and contextualise the Belgian judgement. At the EU level, the attribution of APT 31 is the only common thread explicitly linking the unilateral Belgian declaration of 18 July 2022 to the EU declaration of 19 July 2021.

From the Belgian Government's perspective, its unilateral declaration and public attribution assessment is clear. Back in May 2021, Belgium's National Cybersecurity Strategy established the Government's attribution procedure in which the MFA was given the responsibility for the 'coordinated or uncoordinated international attribution of

[20] European Council (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', 19 July.

[21] Poliisi (2021) 'Eduskunnan tietojärjestelmiin kohdistuneen tietomurron tutkinnassa selvitetään yhteyttä APT31-toimijaan', 18 March; SUPO (2021) 'Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi', 18 March.

[22] Oyvind Bye Skille et al. (2021) 'For første gang sier PST at Kina står bak et dataangrep', 17 June.

[23] BfV (2022) 'Cyber-Brief Nr. 01/2022 – Hinweis auf aktuelle Angriffskampagne', 26 January, pp. 2–3.

[24] ICRC (2022) 'Cyber-attack on ICRC: What we know', 22 June.

[25] Victor Vrabie (2021) 'NAIKON – Traces from a Military Cyber-Espionage Operation', Bitdefender, n.d.; Michael Mimoso (2015) 'Naikon APT Group Tied to China's PLA Unit 78020', *ThreatPost*, 24 September.

malicious cyber activities.'[26] In an email to the author on 20 July 2022, the MFA further explained that 'it has been assessed that the combination of two major incidents related to actors from the same country deserved a public attribution.' The MFA went on to state that 'we are in close contact with our EU partners on this issue and it is foreseen to inform the EU Working Group Cyber [HWPCI] of this national attribution. We will further discuss with our EU partners any possible activation of tools for answering to cyberattacks.'

The MFA's explanation is curious: on the same day the Government released its unilateral declaration, the foreign ministers of the EU's 27 Member States met in Brussels for the monthly meeting of the Foreign Affairs Council (FAC). Chaired by the EU's High Representative for Foreign Affairs and Security Policy, Josep Borrell, the FAC is responsible for the EU's external action. Belgium's declaration did not make it onto the FAC agenda or the final readout.[27] In itself, this omission is not necessarily surprising, since the FAC rarely covers cyber-specific issues. However, when combined with the fact that the Belgian declaration received almost no public support from the other 26 Member States, it looks strange. Apart from three Member States, there was silence across the EU. The Estonian MFA tweeted that 'Estonia supports @BelgiumMFA's request to Chinese authorities to take action against malicious cyber activities by Chinese actors. Estonia strongly supports & stands for the responsible state behaviour online to ensure open, free, secure internet.'[28] The Luxembourg MFA briefly noted that '#Luxembourg stands with #Belgium and supports request to Chinese authorities to take action. We advocate responsible behaviour in #cyberspace.'[29] Lastly, German Cyber Ambassador Regine Grienberger stated that '#GER stands with #BEL in condemning malicious cyber activity and continuing to call upon all states to adhere to the #norms of responsible state behaviour in cyberspace. Together with our partners we will counter cyber threats and build up our common resilience #UNCyberOEWG.'[30] The Belgian declaration also went unnoticed outside the EU. None of the governments of the US, the UK, Canada, Australia or New Zealand publicly acknowledged its existence.

In terms of its content, there does not seem to be anything particularly controversial about the Belgian declaration, which might otherwise have accounted for its muted reception among the country's allies and partners across the globe. The declaration clearly states that the malicious cyber activities 'significantly affected [Belgium's] sovereignty, democracy, security and society at large,' and strongly denounces the campaigns as being 'undertaken in contradiction with the norms of responsible state behaviour as endorsed by all UN Member States.' Notably, however, the MFA stopped short of directly accusing Beijing of cyber espionage and instead 'urged Chinese

[26] CCB (2021) 'Cybersecurity Strategy Belgium 2.0 – 2021-2025', Centre for Cyber Security Belgium, May, p. 38.

[27] Council of the European Union (2022) 'Provisional Agenda: Foreign Affairs – 18 July 2022', 15 July; Council of the European Union (2022) 'Foreign Affairs Council – Brussels, 18 July 2022', July 15.

[28] Estonian MFA (2022) Twitter post, 19 July.

[29] Luxembourg MFA (2022) Twitter post, 20 July.

[30] Regine Grienberger (2022) Twitter post, 26 July.

authorities to take action against malicious cyber activities undertaken by Chinese actors.' [31]

Time will tell whether the Belgian Government will push for a response at the EU level by tabling the declaration for discussion by the Council of the European Union's Horizontal Working Party on Cyber Issues (HWPCI). The HWPCI is responsible for the Council's work on cyber issues, including ensuring a unified approach on cyber policy, information sharing, and legislative activities. At the time of writing, the declaration does not appear to have been discussed within the HWPCI.

If the Belgian Government tables the item and is successful in swaying the other 26 Member States, we will see an EU declaration and potentially other measures in response to the breach of the Belgian MoD and FPS Interior. Such a response will likely be perceived as a positive political endorsement of Belgium's intelligence capability and national attribution process. In contrast, if the Belgian Government fails and the evidence gathered is unable to convince other Member States, this could create political repercussions that will require significant adjustments to Belgium's national attribution process. In other words, any HWPCI discussion will be far from a mere formality with a predictable outcome. Some Member States might even perceive it as being unwise to call out Beijing amid the ongoing geopolitical confrontation with Russia just to score a few irrelevant normative points, while others might seek to utilise the Belgian declaration to further confront Beijing on a host of related issues.

Russian DDoS – 19 July 2022

Roughly 24 hours after the Belgian declaration was published, the EU High Representative for Foreign Affairs and Security Policy released a declaration on behalf of the EU and its Member States on 'malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine.'[32] This marked the third time the EU has published a cyber-related declaration in 2022. The first, on 14 January, strongly condemned the cyberattacks (ie, Russian deployment of wipers) against Ukraine.[33] the second, on 10 May, strongly condemned the 'malicious cyber activity conducted by the Russian Federation against Ukraine, which targeted the satellite KA-SAT network, owned by Viasat.'[34]

[31] Belgian MFA (2022) 'China: Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors', 18 July.

[32] Council of the European Union (2022) 'Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine', Press Release, 19 July.

[33] Council of the European Union (2022) 'Ukraine: Declaration by the High Representative on behalf of the European Union on the cyberattack against Ukraine', Press Release, 14 January.

[34] Council of the European Union (2022) 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', Press Release, 10 May.

The discussion by the HWPCI on the EU's third declaration likely commenced on 8 July under the agenda item 'Cyber Diplomacy Toolbox.'[35] However, the specific event that triggered the decision to publish an EU declaration remains unclear. One reading is that the cumulative DDoS campaigns of pro-Russian hacktivist groups against the digital infrastructure of several EU Member States reached a political turning point at the beginning of July. Another reading is that KillNet's 10-day DDoS campaign against Lithuania, which was initiated on 20 June in reaction to Vilnius banning the transit of goods by rail between Russia and Kaliningrad, forced the Council of the European Union into action.

The available public evidence underlying the cumulative narrative is lacking in strength. On 1 May, Legion – KillNet's DDoS special operations team – targeted several government sites in Lithuania, Moldova and Latvia.[36] On 2 May, it conducted DDoS campaigns against the websites of the German police, taxi services and a handful of German companies.[37] On 8 May, Legion carried out DDoS attacks on several sites in Poland, including mBank, the police and the University of Warsaw, as well as some sites in Romania. On 10 and 11 May, Legion went on to carry out a DDoS attach on the website of the Eurovision song contest with limited success. And on 16 May, KillNet officially declared war on ten countries: Estonia, Germany, Italy, Latvia, Lithuania, Poland, Romania, Ukraine, the US and the UK. At this particular point in time, the EU was already in a position to publish a declaration on pro-Russian DDoS campaigns against multiple EU Member States, but it refrained from doing so. The underlying logic may have been that these DDoS campaigns did not result in any substantive disruptive effects and therefore did not warrant a political reaction.

On the other hand, if we accept the notion that KillNet's 10-day campaign against Lithuania was an inflection point, then certainly it must have had a substantial disruptive effect. On the one hand, according to Jonas Skardinskas, acting director of Lithuania's National Cyber Security Centre, more than 130 websites were 'hindered' or rendered inaccessible during that period.[38] On the other hand, Vice Minister of National Defence Margiris Abukevičius stated on 27 June that the DDoS had 'limited success': while KillNet managed to take down a number of sites, the Government was soon able to restore them.[39] Depending on the viewpoint, KillNet's campaign was either the worst cyberattack Lithuania has ever experienced or a non-event that resulted in minor inconveniences. Looking at it from the outside, it thus remains unclear whether the EU Member States

[35] Council of the European Union (2022) 'Notice of Meeting and Provisional Agenda: Horizontal Working Party on Cyber Issues', 6 July; Council of the European Union (2022) 'Notice of Meeting and Provisional Agenda: Horizontal Working Party on Cyber Issues', 12 July;

[36] Legion (2022) Telegram Post- Lithuania, 1 May; Legion (2022) Telegram Post - Moldova, 1 May; Legion (2022) Telegram Post - Latvia, 1 May.

[37] Legion (2022) Telegram Post – Germany (1), 2 May; Legion (2022) Telegram Post - Germany (2), 2 May; Legion (2022) Telegram Post – Germany (3), 2 May; Legion (2022) Telegram Post – Germany (4), 3 May; Legion (2022) Telegram Post – Germany (5), 3 May; Legion (2022) Telegram Post – Germany (6), 4 May; Legion (2022) Telegram Post – Germany (7), 5 May.

[38] Matt Burgess (2022) 'Russian 'Hacktivists' Are Causing Trouble Far Beyond Ukraine', *Wired*, 11 July.

[39] Antoaneta Roussi and Laurens Cerulus (2022) 'Russian hackers attack Lithuania over Kaliningrad sanctions', *Politico*, 27 June.

maintain a principled approach on whether and when to publish a EU declaration or whether this depends on pressure from individual Member States.

In line with the Belgian declaration, the EU's declaration on 19 July did not attribute KillNet's conduct to the Russian state. Instead, it called upon 'all states to comply with their due diligence obligations and urge[d] them to take appropriate actions against malicious cyber activities conducted from their territory.'[40] Essentially, the Council pointed to the exact same United Nations norms of responsible state behaviour and due diligence obligations as the Belgian declaration the day before. Yet, the public reaction from both the EU Member States and the Five Eyes alliance was markedly different this time round.

All in all, 13 Member States publicly reacted to the release of the EU declaration. Ten condemned the DDoS attacks on Twitter, including Austria, the Czech Republic, Denmark, Estonia, Finland, Latvia, Lithuania, the Netherlands, Poland and Slovenia. For example, the Austrian MFA tweeted that 'We are deeply concerned about the increase in cyberattacks in the context of #Russia's military aggression against #Ukraine. All states must take action against malicious cyber activities conducted from their territory.'[41] The Slovenian MFA noted that 'Slovenia strongly condemns malicious cyber activities directed against #EU and partner countries, and calls for responsible behaviour of countries in cyberspace.'[42] The Polish MFA even released a written statement on its website which explained that 'Pro-Russian hackers have taken responsibility for carrying out these attacks, which not only support Russia's military efforts, but also target the countries that provide the biggest assistance to the defending Ukraine - including Poland.'[43] Three countries (Ireland, Romania and Slovakia) retweeted the statement made by Josep Borrell, and 14 remained silent – among them Germany, France, Spain, Sweden and, curiously, Belgium. Neither the Belgian MFA, the Permanent Representation of Belgium to the EU nor Foreign Minister Hadja Lahbib – who assumed office only four days earlier on 15 July – publicly reacted to the EU declaration.

Outside the EU, all Five Eyes members endorsed the EU declaration. The UK Foreign Commonwealth and Development Office tweeted that 'cyberattacks orchestrated by pro-Russian criminal groups against UK allies since Russia invaded Ukraine are unacceptable. This is just one example of the growing threats facing democracies.'[44] US Secretary of State Antony Blinken proclaimed that 'we stand with the EU, Ukraine, and all victims of malicious cyber activity during Russia's unjustified and unprovoked war against Ukraine. The Russian Government must uphold its commitments to international

[40] Council of the European Union (2022) 'Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine', 19 July.

[41] Dutch MFA (2022) Twitter post, 19 July; For the complete dataset see: https://docs.google.com/spreadsheets/d/1ILRYfDwNCsSvT6N5Ky87PfuABKsCJKOx_-vTKyotZro/edit?usp=sharing

[42] Slovenia MFA (2022) Twitter post, 19 July.

[43] Polish MFA (2022) 'MFA statement condemning cyberattacks of pro-Russian hacker groups', gov.pl, 19 July.

[44] United Kingdom, Foreign, Commonwealth and Development Office (2022) Twitter post, 19 July.

norms and bring the perpetrators to justice.'[45] Canada's Foreign Minister Melanie Joly explained that 'Canada stands with you @JosepBorrellF in condemning Russian Cyberattacks and threatening the legitimacy of critical infrastructures. We will continue to work with our European counterparts to prevent and counter future malicious cyberattacks.'[46] And Australia's Assistant Minister of Foreign Affairs Tim Watts declared that 'recent cyberattacks conducted by pro-Russian hacker groups are yet another example of the increasing cyber threats in the context of Russia's aggression against Ukraine. Australia will continue to work with partners to prevent and counter malicious cyberattacks.'[47] Australia's particularly strong reaction was rather unusual, as one would assume that from a purely geopolitical and normative reasoning, the Chinese APT campaigns against Belgium would be of a much higher political priority to Canberra than pro-Russian hacktivists carrying out DDoS attacks on a handful of EU Member States. Yet, reflecting the current geopolitical focus on Russia, even New Zealand's Ministry of Foreign Affairs and Trade stated that 'Aotearoa New Zealand condemns all malicious cyber activity. We stand with our European counterparts in a strong condemnation of cyberattacks against Ukraine, and essential entities worldwide.'[48].

Conclusion

The discrepancies between the widespread political support for the EU's declaration and the absence of public support for the Belgian one does not necessarily come as a surprise. However, the concern is that it might result in significant dissonance on a more fundamental level as a result of the EU's selective politicisation of whether and when to emphasise norms and rules for state behaviour in cyberspace.

Nonetheless, one could argue that this is a minor issue. Maybe the Belgian Government simply did not inform any of its allies and partners prior to publishing the declaration calling out Beijing. However, according to the Belgian MFA, this was not the case. In an email to the author on 20 July, the ministry explained that 'we are in close contact with our EU partners on this issue and it is foreseen to inform the EU Working Group Cyber [HWPCI] of this national attribution. We will further discuss with our EU partners any possible activation of tools for answering to cyberattacks.' Similarly, the Belgian declaration should not have come as a surprise to any of the EU Member States given that: (a) the malicious campaigns were discovered in 2021; and (b) Belgium's National Cybersecurity Strategy of May 2021 set out the national attribution procedure, giving the MFA responsibility for the 'coordinated or uncoordinated international attribution of malicious cyber activities.'[49] As a case in point, it would have been rather awkward if Belgium's new national attribution procedure failed to trigger after discovering several APTs in the networks of two government ministries.

[45] US Secretary of State, Antony Blinken (2022) Twitter post, 20 July.

[46] Canadian Foreign Minister, Melanie Joly (2022) Twitter post, 19 July.

[47] Australian Assistant Foreign, Minister Tim Watts (2022) Twitter post, 20 July.

[48] New Zealand MFAT (2022) Twitter post, 20 July.

[49] CCB (2021) 'Cybersecurity Strategy Belgium 2.0 – 2021-2025', Centre for Cyber Security Belgium, May, p. 38.

Overall, there are numerous signs that the geopolitical shift caused by the Russian invasion of Ukraine has resulted in deliberate inconsistencies in Member States' applications of international law governing cyberspace and adherence to the United Nations cyber norms framework. One symptom of this is the lack of public support for the Belgian declaration and the over-reaction to the DDoS campaigns by pro-Russian groups. Another symptom is the calculated disregard of the conduct of the IT Army of Ukraine (led by the Ukrainian Government), including its usage of digital infrastructure in EU Member States, as well as the active participation of EU citizens, people, and companies located on EU territory to conduct DDoS campaigns against Russian civilian and government infrastructure over the past eight months.[50] The EU's continued silence on the IT Army's conduct is at odds with Member States' own due diligence obligations under international law.

Moving forward, these developments do not bode well for the EU's consistent application of international law and norms and rules for responsible state behaviour in cyberspace. Hopefully, the EU and its Member States will address these discrepancies in the near term by reacting to Belgium's unilateral declaration and clarifying the EU's legal positions on the IT Army in a domestic and international context. That said, while deliberately eroding the already fragile consensus on international law and norms and rules for state behaviour in cyberspace may accommodate current geopolitical rationales in many EU Member States, there is a strong chance this will prove detrimental to European security in the years and decades ahead.

[50] Stefan Soesanto (2022) 'The IT Army of Ukraine Structure, Tasking, and Ecosystem', Center for Security Studies, ETH Zurich, June.