The limits of like-mindedness in cyberspace

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

Tema

In reaction to the Ghostwriter campaign, the EU's High Representative for Foreign Affairs and Security Policy, Josep Borrell, published a Declaration on 24 September 2021 on the 'respect for the EU's democratic processes'. Surprisingly, the Declaration inherently failed to rally widespread public support among Western democracies in Europe and beyond.

Resumen

The EU High Representative's Declaration on Ghostwriter stands out as the perfect case study to fundamentally examine whether like-mindedness in cyberspace actually exists among Western democracies. This paper will show that like-mindedness was not on display on 24 September, and it will explain that strategic miscalculations, legal inaccuracies and political bargaining failures within the EU's decision-making process are likely to blame for the Declaration's poor result.

Análisis

One Declaration of many?

Within the context of the EU's cyber diplomacy toolbox, the September Declaration was the third by the High Representative (HR) in 2021.[1] The HR has issued seven Declarations overall, including on Solarwinds, the coronavirus pandemic, China and other topics. All the Declarations speak on behalf of the EU and the 27 member states and, given the absence of a collective attribution mechanism at the EU level, naturally focus on norms and international law applicable to cyberspace.

The 24 September Declaration stands out for being rather short, at just 168 words. The word count of all previous cyber-related Declarations hovers between 277 and 379 words, an average of 355, which is more than double the length of the September one. It is unclear why it was kept that short, but it was likely influenced by two factors: the need to publish the Declaration before the German Federal Election on 26 September, and the political consensus that could be achieved between the 27 member states on the specific content and language used. Speaking to Politico's *National Security Daily*, the EU Council's spokeswoman Nabila Massrali elaborated that 'the EU felt the need to

[1] EU Declaration (2021), Press Release, 24/IX/2021; The first was published on 'expressing solidarity with the United States on the impact of the SolarWinds cyber operation', Press Release, 15/IV/2021; and the second urged 'Chinese authorities to take action against malicious cyber activities undertaken from its territory', Press Release, 19/VII/2021.

put out a statement after Germany, in the course of normal discussions, declared it was under cyberthreat from Russia'.[2]

The discussion on the HR's Declaration was likely introduced into the EU Council's Horizontal Working Party on Cyber Issues (HWPCI) on 15 September under the agenda item 'Cyber Diplomacy Toolbox'. Two subsequent HWPCI meetings on 17 and 22 September resulted in commencing the Council's silent procedure and allowed the subsequent publication of the Declaration on the 24th. Thus, the Declaration was adopted within nine days.

Contrasting this with the HR's 15 April Declaration on SolarWinds, for instance, the speed of the HWPCI procedure was not unusual. The discussion on the SolarWinds Declaration was introduced to the HWPCI on 18 March –also under the agenda item 'Cyber Diplomacy Toolbox'–. Three subsequent meetings were held on the topic on 22, 24 and 26 March.[3] Overall, it took the HWPCI just eight days to arrive at a consensus.

Looking back at the HR's four Declarations in 2019 and 2020, it can easily be seen that they were all phrased in very general terms by, for instance, urging 'actors to stop undertaking such malicious activities' and expressing 'concern about the cyber-attack' against Georgia. Thus, they never called out specific actors or governments as threats, nor were they used for public attribution purposes. This slowly changed in 2021, with the 15 April Declaration noting that 'the SolarWinds cyber operation, which, the United States assesses, has been conducted by the Russian Federation'.[4] While the EU did not put forward its own attribution assessment on SolarWinds, it was nonetheless unprecedented for the HR to cite a third-party attribution assessment –particularly by a non-EU member state–. The HR's Declaration of 19 July on China pushed this move further along by mentioning for the first time ever two specific Chinese threat actor groups (APT40 and APT31) that have been targeting 'government institutions and political organisations in the EU and member states, as well as key European industries'.[5] While the 19 July Declaration abstained from establishing a direct attribution link between these groups and the Chinese government –by merely stating that these activities 'have been conducted from the territory of China'– the Declaration inched much closer to a collective EU attribution statement than any previous Declaration.

The 24 September Declaration is the latest progression in this process by stating that 'some EU Member States have observed malicious cyber activities, collectively designated as Ghostwriter, and associated these with the Russian state'. The only tweaks that would be necessary to turn this Declaration into a collective EU attribution statement would be to change the word 'some' into 'all' EU member states and move from 'associated these [activities] with' to 'attributed these [activities] to the Russian state'. It might even be sufficient to merely point to a 'majority' of EU members states if (a) the voting mechanism in the EU Council on actions taken within the context of the

[2] Alexander Ward (2021), 'Progressive foreign policy's big week', *Politico*, 24/IX/2021.

[3] HWPCI (2021), CM 2283/21, 16/III/2021; CM 2342/21 and CM 2343/21, 18/III/2021; and CM 2410/21, 25/III/2021.

[4] EU Declaration (2021), Press Release, 15/IV/2021.

[5] EU Declaration (2021), Press Release, 19/VII/2021.

EU cyber diplomacy toolbox is changed to qualified majority voting –as envisioned in the EU's Cybersecurity Strategy for the Digital Decade–, and (b) if the EU moves away from viewing attribution as a sovereign political decision towards a national prerogative of the individual member states. It remains to be seen whether the EU Council will make the final leap. Given the current trajectory, the next HR Declaration could very well turn into a collective EU public attribution statement.

Ghostwriter targeting Poland and Lithuania

Published in July 2020, Fireye/Mandiant's first report on Ghostwriter assessed with moderate confidence that the activity set they identified –based on 14 incidents– was part of a broader influence campaign that has been going on since at least March 2017.[6] While FireEye did not attribute the campaign to a specific threat actor, the activity set's behaviour was 'aligned with Russian security interests, primarily seeking to foment distrust of US and NATO troops in Europe by portraying their presence as aggressive and dangerous to local populations and to undermine military relations between NATO members'. Ghostwriter's targets between March 2017 and May 2020 included Poland, Lithuania and to some extent Latvia. In terms of tactics, Ghostwriter's preference was to leverage 'website compromises or spoofed email accounts to disseminate fabricated content' and leverage 'multi-use inauthentic personas with developed histories, or single use personas impersonating real individuals or behind which at least some effort has been made to make them appear authentic, on a specific set of core platforms'. As FireEye carefully explains, this tactical behaviour makes Ghostwriter's activity distinctly different from the supposedly Russian influence campaign known as 'Secondary Infektion', which has been exposed over the years.[7] The Polish government's initial reaction to the Ghostwriter campaign was limited to combatting the spread of disinformation by releasing official government statements on 23 April and 28 May 2020.[8]

Mandiant's second report, published in April 2021, detected an additional 20 operations that fit Ghostwriter's activity set, pushing the campaign's earliest discovery back to 8 July 2016.[9] Out of these 20 operations, 10 were aimed at Poland, seven at Lithuania and the rest at Ukraine and the Baltics in general. Almost all of the operations aimed at Poland were detected between October 2020 and March 2021. Mandiant concluded that Ghostwriter expanded its narratives and targeting processes by 'heavily leverag[ing] the compromised social media accounts of Polish officials on the political right to publish content seemingly intended to create domestic political disruption in Poland rather than foment distrust of NATO'. Notably, Mandiant also explained that based on recently obtained technical evidence, they now 'assess with high confidence that UNC1151, a suspected state-sponsored cyber espionage actor that engages in credential harvesting and malware campaigns, conducts at least some components of Ghostwriter influence activity'.

[6] FireEye/Mandiant (2020), 'Ghostwriter Influence Campaign', July.

[7] DFRLab (2019), 'Operation Secondary Infektion', Atlantic Council, 22/VI/2019.

[8] Gov.pl (2021), 'Atak dezinformacyjny na Polskę', 23/IV/2021; Gov.pol (2021), 'Kolejny atak informacyjny na Polskę', 28/V/2021.

[9] Fireye/Mandiant (2021), 'Ghostwriter update', April, p. 14.

In early June, the Polish Prime Minister's chief of staff Michał Dworczyk reported to the state services that he and his wife's private email and social media accounts had been broken into. Email conversations from Dworczyk's inbox subsequently appeared on two Telegram channels.[10] Dworczyk offered his resignation to Prime Minister Morawiecki, who refused, saying that he had not lost confidence in him. The incident kicked off a host of government meetings as the sheer size of the phishing campaign became apparent. On 16 June, government spokesperson Piotr Mueller noted in a press conference that 'in the coming weeks, the whole of Poland, as a political class, regardless of political colours, we will be the subject of a disinformation attack'.[11] Two days later, Poland's ruling party leader, Jarosław Kaczyński, released a written statement to the effect that 'Poland's top officials, ministers, lawmakers of various political stripes were subject to a cyber attack. […] The analysis of our services and the special services of our allies allows for a clear statement that the cyberattack was carried out from the territory of the Russian Federation'.[12] On the same day, Prime Minister Morawiecki said that Poland's security services were scrambling to 'secure the many inboxes' of ranking politicians victimised by an 'external hack cooked up at the Kremlin'.[13] On 22 June 2021 Stanislaw Zaryn, spokesperson for the Minister coordinating Poland's Special Services, put out a written statement explaining that 4,350 Polish email users –of which over 100 accounts belonged to current and former government officials– were the target of a recent social engineering attack. Poland's Internal Security Agency and the Military's Counterintelligence Service assessed that UNC1151 was responsible for the attacks, and that it was part of the Ghostwriter campaign.[14] The statement goes on to note that 'the secret services have reliable information at their disposal' that connects UNC1151 to 'the activities of the Russian secret services'.

According to Polskie Radio, 'in June, after the attack, Poland requested a response from the European Union using its cyber diplomacy toolbox'.[15] Warsaw notably sought condemnation of the attacks during the European Council summit on 24-25 June. Indeed, the EU Summit's conclusion does include one item that broadly 'condemns recent malicious cyber activities against Member States, including in Ireland and Poland. It invites the Council to explore appropriate measures within the framework of the cyber diplomacy toolbox'.[16]

The GhostWriter campaign against Poland might have been subsequently discussed in the HWPCI on 28 June, 7 July and 13 July –under the agenda item 'Cyber Diplomacy Toolbox: Discussion'–.[17] The topic disappeared from the HWPCI agenda afterwards with no action taken at the EU level. From the outside, it seemed that Warsaw was unable to

[10] Ana Wolska (2021), 'More emails of Poland's PM office head Dworczyk leaked', 16/VI/2021.

[11] Piotr Mueller (2021), 'Poland faces disinformation campaign says gov' spokeperson', Polish Press Agency, 16/VI/2021.

[12] Gov.pl (2021), 'Oświadczenie Wiceprezesa Rady Ministrów Przewodniczącego Komitetu ds. Bezpieczeństwa Narodowego i spraw Obronnych Jarosława Kaczyńskiego', 18/VI/2021.

[13] RFERL (2021), 'Poles blame Kremlin for "unprecedented" cyberattack on senior officials', 19/VI/2021.

[14] Gov.pl (2021), 'Findings regarding hacker attacks', 22/VI/2021.

[15] Radio Poland (2021), 'EU slams Russia for cyberattacks', 25/IX/2021.

[16] European Council (2021), Conclusions EUCO 7/21, 25/VI/2021.

[17] HWPCI (2021), CM 2780/21, 25/VI/2021; CM 3867/2/21 Rev2, 6/VII/2021; CM 3989/21, 12/VII/2021.

achieve a political consensus on the shared situational awareness among the 27 member states. It is unclear why that was the case, but according to a senior EU Commission official cited by Politico, 'the information [Poland] passed [to the EU] didn't shed new light on the [attribution] situation'.[18] If true, then the Polish government either did not pass all the relevant intelligence on Ghostwriter to the EU, or the EU members deemed the quality of the intelligence supplied by Warsaw sub-par. These issues notwithstanding, in hindsight, the HWPCI's decision to do nothing at all was likely a political mistake. The failure to act does open up the question as to whether the intelligence sharing and political bargaining process underlying the EU cyber diplomacy toolbox is politically unworkable for some EU countries. In addition, it raises doubts as to whether the Union's aspiration of a common EU threat perception and situational awareness in cyberspace is actually able to objectively reflect the geopolitical realities as perceived by the individual member states.

Warsaw also apparently took the Ghostwriter issue to NATO. On 18 June, the Ministry responsible for the coordination of Poland's Special Services noted that 'I would like to inform you that the Internal Security Agency sent to the special services of NATO member states information on cyberattacks carried out against Poland'.[19] The following day the Polish Press Agency quoted a NATO HQ source saying that the North Atlantic Council 'will discuss the matter, probably next week'.[20] It is unknown whether the meeting actually took place or whether any conclusions were reached as NATO never released a public statement on Ghostwriter.

Ghostwriter targeting Germany

In contrast to Poland's fruitless efforts on the EU level, the German course of action yielded very different results. On 26 March 2021 the German news magazine *Der Spiegel* reported that seven members of Parliament and 31 members of various state parliaments were targeted by a phishing campaign suspected to be conducted by Ghostwriter. According to *Der Tagesspiegel*, the campaign was run against the parliamentarians' private GMX and T-online email accounts rather than their official Bundestag ones. The German Federal Office for the Protection of the Constitution (BfV) and the Federal Office for Information Security (BSI) detected the phishing campaign early on and informed potential victims.[21] Ghostwriter apparently did not stop its phishing campaigns over the subsequent months and even increased its efforts at the end of August in the run up to the German federal election on 26 September.

In early September the German government had enough. State secretary Miguel Berger passed a protest note directly to the Russian Deputy Foreign Minister Vladimir Titov at a meeting of the German-Russian High Working Group on Security Policy. And Andrea Sasse –spokeswoman for the German Foreign Ministry– publicly confirmed that a protest was lodged and acknowledged for the first time that 'the German government has reliable information on the basis of which Ghostwriter activities can be attributed to cyber-actors

[18] Zosia Wanat (2021), 'Leaked email scandal engulfs Poland's political elite', *Politico*, 24/VI/2021.

[19] Gov.pl (2021), 'Findings regarding hacker attacks', 22/VI/2021.

[20] PAP.pl (2021), 'NATO to investigate cyber-attacks on Poland', 19/VI/2021.

[21] Der Tagesspiegel (2021), 'Russische Hacker schicken deutschen Politikern Phishing-Mails', 26/III/2021.

of the Russian state and, specifically, Russia's GRU military intelligence service'.[22] Later, *Tagesschau* exclusively reported that the German Public Prosecutor General opened up a preliminary investigation into the Ghostwriter attacks based on a dossier compiled by the BfV, which assessed with a high degree of confidence that the GRU is behind the Ghostwriter campaigns targeting Germany.[23] On 15 September the Ghostwriter issue was introduced into the HWPCI and nine days later the EU High Representative published his Declaration. As the time of writing, it is unknown whether Ghostwriter successfully breached any inboxes of the targeted German politicians. In contrast to Poland, so far, no examples have publicly surfaced in Germany of Ghostwriter leaking emails, compromising websites, spoofing accounts or disseminating fabricated content.

Aftermath and like-mindedness

As far as the Polish Ministry of Foreign Affairs is concerned, the official narrative is that 'in June, Poland requested that the EU use its cyber diplomacy tools. Germany addressed a similar request in early September. These steps have resulted in the EU Declaration published today […]'.[24] The Polish Permanent Representation to the EU put it even more bluntly by tweeting on 24 September that 'at our request, Russia's cyberattacks and disinformation activities aimed at Poland and other EU countries evoke a strong response'.[25] Given the timeline in question and the evidence at hand, it is almost certain that Warsaw is trying to portray itself as the primary mover at the EU level that led to the publication of the HR's Declaration –even though it was not–.

Interestingly, the Texas-based threat intelligence company Prevailion published a report on 1 September 2021, which identified 83 previously unknown domains as being part of UNC1511's campaign. Prevailion separated the domains into two clusters: 52 domains that it assesses with high confidence to be part of the UNC1511 infrastructure, and 31 domains with moderate confidence.[26] While the high confidence cluster 'appears designed to capture login credentials for official and personal accounts of Polish and Ukrainian audiences', it also included phishing domains that 'were intended to gain login credentials for members of the French Defence Ministry's DICoD [Data, Information and Communication Digital service]'.[27] At the time of writing, it is unknown whether any accounts of French defence personnel were successfully breached by UNC1151. It is also unclear whether the French government took a particularly strong view of Ghostwriter when the issue was raised by the Germans in the EU Council. Given that the GRU notably targeted President Macron's political party in the run up to the 2017 French presidential election, it could be presumed that the German push for a Declaration in the run up to the German federal election was supported by Paris.[28] Judging the French government by the behaviour of its official social media accounts,

[22] Geir Moulson (2021), 'Germany protests to Russia over pre-election cyberattacks', AP News, 6/IX/2021.

[23] Florian Flade (2021), 'Verfahren wegen Hackerattacken', *Tagesschau*, 9/IX/2021.

[24] Gov.pl (2021), 'Polish MFA statement', 24/IX/2021.

[25] https://twitter.com/PLPermRepEU/status/1441352154388869120.

[26] Prevailion (2021), 'Diving deep into UNC1151's infrastructure: Ghostwriter and beyond', 1/XI/2021.

[27] Ibid.

[28] United Stated District Court (2020), 'United States of America v. Yuriy Sergeyevich Andrienko *et al*.', Western District of Pennsylvania, 15/X/2020, p. 3.

however, then its utter silence when the HR published his Declaration on 24 September points toward political indifference rather than a strong sentiment on Ghostwriter. Neither the Twitter accounts of the French Ministry of Foreign Affairs, the Ministry of Defence, the French Representation at the EU, the Office of the Ambassador for Digital Affairs or the individual accounts of the French ministers and ambassadors retweeted, liked or commented on the HR's Declaration.[29]

Based on a comprehensive analysis of the official Twitter accounts of all the 27 EU member states, we know that 10 member states posted a supporting tweet, three merely retweeted the HR's Declaration (Estonia, Germany and Ireland), two published a written statement on their respective government websites (Poland and Slovenia) and 12 member states remained completely silent. By comparison, in reaction to the HR's Declaration on 19 July on China, 14 posted a tweet in support, four simply retweeted the Declaration (Croatia, France, Germany and Ireland), two published a written statement (Estonia and Romania) and only nine remained completely silent.

It is entirely unclear why exactly some member states choose to be more vocal on one Declaration than on others. Notably, the Slovenian government, which currently holds the rotating EU Council Presidency, published a supporting tweet on 19 July and on 24 September. However, on 24 September it additionally published a very short written statement on the Foreign Ministry's website. No written statement was published on 19 July. The Estonian and Romanian governments did the opposite, publishing written statements on 19 July, while merely retweeting the HR's Declaration on 24 September. Meanwhile, the German government has been consistent throughout by only retweeting the HR's Declaration on 19 July and 24 September, even though the latter only materialised because the German Foreign Ministry strongly pushed for an EU response. In contrast to Germany's consistency, the Polish Ministry of Foreign Affairs published a 313-word long written statement on its website on 24 September, while only publishing a supporting tweet on 19 July.

The Confusion

Some of the differences in the public support visible on Twitter might stem from whether governments perfectly or partially align with the Declaration's content and focus. This means that even though the discussion in the HWPCI is trying to make every member state as happy as possible, differences in language, terminology used, priorities and assertions made might have been waved through for the sheer sake of achieving political agreement. We can identify several oddities in the September Declaration that could explain the Twitter behaviour of the different member states.

First, instead of clearly mentioning which EU member states were affected by Ghostwriter, the Declaration only points to 'some EU member states'. This disguises the true extent of the adversarial campaign and diffuses the importance of the EU's reaction. The same logic also holds true for the Declaration's notion that member states 'associated these activities with the Russian state'. A more forceful Declaration could

[29] For information see this database. Philippe Léglise-Costa, the French Permanent Representative to the EU, does not seem to have a Twitter account.

have pointed to the German MFA attributing Ghostwriter to the GRU, and the assessment by Poland's Internal Security Agency and Military Counterintelligence Service that UNC1151's activity is connected to the Russian secret services. If the US attribution assessment on SolarWinds can make it into an EU Declaration then it seems rather odd to ignore the attribution statements of two EU member states.

Secondly, the Declaration strangely states that Ghostwriter's activities are 'contrary to the norms of responsible State behaviour in cyberspace as endorsed by all UN Member States […]'. However, none of the 11 norms outlined by the UN GGE and reaffirmed in the 2021 OEWG final report, touches upon the targeting of democratic institutions and processes, spreading disinformation or stealing data from the personal accounts of government officials. In fact, even if there were such a UN norm to tackle all these different aspects, it would notably be as voluntary and non-binding as all the other UN norms.[30]

Third, the Declaration entirely fails to make any reference to international law, nor does it point to the principle of non-intervention or violation of state sovereignty, which would be a much stronger legal foundation than urging the Russian Federation to adhere to non-binding norms.

And fourth, for the first time ever, a sentence was included to the effect that the 'European Union will revert to this issue in upcoming meetings and consider taking further steps'. This is both encouraging and troubling. It is encouraging because the EU Council essentially commits itself to dig deeper into the Ghostwriter campaign. But it is also troubling because the only other tool left in the EU cyber diplomacy toolbox is cyber sanctions –whose effectiveness and cost imposition tends to be close to zero–.[31]

Like-mindedness outside the EU

Public support for the HR's Declaration outside the EU was very timid. Five of the six European non-EU NATO member states (Montenegro, North Macedonia, Norway, Iceland and Turkey) did not voice any public support for the Declaration. Neither did any of the EFTA countries, nor the governments of Georgia, Ukraine or Japan. Among the Five Eyes countries, four posted a supporting tweet –of which two did not bother to retweet, link or even mention the HR's Declaration itself (the UK and Canada)–. The British Minister for European Neighbourhood & the Americas, Wendy Morton, was the only high-ranking UK government official to post a supporting tweet. Her tweet was notably retweeted by the UK Mission to the EU but was not picked up by the UK FCDO nor received any attention from the British Foreign Secretary, Liz Truss. A similar dynamic played out in New Zealand, with the supporting tweet only being published by the New Zealand Mission to the EU, which has a mere 992 followers. Given that the US-

[30] Swiss Federal Department of Foreign Affairs (2021), 'Eleven norms of responsible state behaviour in cyberspace', 7/IV/2021.

[31] Stefan Soesanto (2021), 'Europe has no strategy on cyber sanctions', *Lawfare*, 20/XI/2021.

EU Cyber Dialogue was held on 22 September 22, it should come as no surprise that US Secretary of State Blinken published a supporting tweet as well.[32]

By contrast, Australia's Minister for Foreign Affairs, Marise Payne, posted not only a supporting tweet but also released a 198-word long statement on the Foreign Ministry's website. Ironically, the Australian statement is 30 words longer than the HR's Declaration itself, stresses the importance of international law and even goes so far as to note that 'Australia is committed to cooperating with our international partners, including the EU, to deter and respond to malicious cyber activities […]'.[33] Notably, none of the Five Eyes mentions the attribution of Ghostwriter to the Russian state in their tweets and statements.

Conclusiones

From the outside looking in, it might be assumed that a HR Declaration that calls out malicious cyber activities threatening the 'integrity and security, democratic values and principles and the core functioning of [EU] democracies' would receive widespread public support among the EU member states and Western-style democracies around the globe. As this paper has shown, that assumption is false. Overall, the HR's Declaration on Ghostwriter stands out as the perfect case study to fundamentally question whether like-mindedness in cyberspace actually exists among democracies. If it does exist, then it was certainly not on display on 24 September.

One can also only hope that the EU and the member states will (a) re-visit the political decision-making process within the HWPCI, (b) examine the logic of pushing out a Declaration without any reference to international law, (c) start to include attribution assertions made by the member states affected, and (d) coordinate vocal public support for any Declaration, particularly those calling out malicious campaign that undermine the functioning and integrity of democratic processes.

[32] See https://twitter.com/SecBlinken/status/1441433540512690177 and https://twitter.com/State_Cyber/status/1440457861297958919.

[33] Senator the Hon. Marise Payne (2021), 'Australia stands in solidarity with the EU against malicious cyber activity', Australian Minister for Foreign Affairs/Minister for Women, 24/IX/2021.