NIDS 防衛研究所 National Institute for Defense Studies
NIDS Commentary
No. 224 May 26, 2022
(Updated: October 31, 2023*)

Weaponized Disclosure of Intelligence in the Russia-Ukraine War

—— Disclosure Dilemma and Hidden Inheritances from post-2014 Transatlantic Security Cooperation

Research Fellow, Cyber Security Division, Policy Studies Department
SETO Takashi

**Notes: This NIDS commentary (No.224) was originally published in Japanese on May 26, 2022. This English version, published on October 31, 2023, is basically translated from the original edition but with a few updates of citations to incorporate the development of the previous studies as well as key strategic documents of the Government of Japan since the date of the original publication.*

Introduction: Is Intelligence Disclosure for Information Warfare?

Russia's full-scale military invasion of Ukraine since February 2022 has continued as the biggest conventional warfare in European theater since the end of WW (hereafter the Russia-Ukraine War). In addition to myriad agendas of warfighting, this war has sparked renewed discussion on the multiple roles of "intelligence"[1] in 21st-century armed conflicts. Especially, strategic declassification and public disclosure of intelligence products (hereafter, "weaponized disclosure") have attracted media and pundits' attention in Japan. Since December 2021, the US and UK have relentlessly exposed Russia's capabilities and intentions of its military invasion, from their military mobilization around the borders to the covert plan to install a pro-Russian proxy regime in Ukraine. While the Cold War history saw rare disclosure of intelligence, the US/UK initiatives have been unprecedented in their volume and speed of disclosure.

The combination of the media coverage of the US/UK efforts and revisited interests in the roles of information in warfighting, as well as peacetime competition, have also shaped Japan's defense planners' attention to weaponized disclosure. In accordance with key defense and strategic documents since December 2022, it has been regarded as one of the toolboxes of "*Integrated Information Warfare with Special Regard to the Cognitive Dimension*." which Defense Intelligence Headquarters (DIH) under the Ministry of Defense is supposed to lead (inter-services) developments of doctrine and capability.[2]

Little dedicated analysis and scholarly discussion, however, has been done in Japan's strategic community

with reflection on the theoretical conundrum and historical continuity of the weaponized disclosure, which could have implications for the future trajectory of the doctrine and capability developments. Against this backdrop, the author shows that the US/UK weaponized disclosure is not in a vacuum from broader theoretical debates of intelligence studies and unique contexts of the Russia-Ukraine War, reflecting a growing body of academic literature and policy-oriented analysis. For this purpose, this commentary elaborates on the following two points.

First, weaponized disclosure has always posed a critical "dilemma" to nation-state intelligence services, which requires them to strike a balance between creating effects by disclosure and controlling the risks of compromising sources and methods for future intelligence collection, scholarly called "disclosure dilemma."[3] It points out that strategic and operational conditions surrounding the Russia-Ukraine War have alleviated the severity of the disclosure dilemma, enabling exceptional scale and speed of their initiatives.

Second, such enabling conditions have arisen from cumulative preparedness through 8 years of the transatlantic security corporation between the NATO allies and like-minded partners. In other words, the US/UK weaponized disclosure has leveraged hidden "inheritances.", which have been shaped through 8 years of collective regional security efforts from February 2014 toward February 2022. As such, the utility of similar initiatives may not be taken for granted in the other conflict modalities. Thus, scholars and practitioners should carefully analyze these attributes of the US/UK's success and possible enablers/constraints surrounding future contingency scenarios.

This NIDS commentary consists of the following blocks. The first section provides the basis for the subsequent discussion by summarizing the four pillars of intelligence-driven security cooperation before and after the full-scale invasion. The author sheds light on their precedents and linkage with allied intelligence-led campaigns against countering Russian hybrid threats in the second half of the 2010s. From Section 2 to Section 4, the author elaborates on the theoretical and practical conundrum of weaponized disclosure in the Russia-Ukraine War and beyond. These sections provide perspectives on the functions and limitations of weaponized disclosure as a policy means while highlighting controversy on the "disclosure dilemma," which challenges the traditional intelligence apparatus's modus operandi and organizational culture. Reflecting theoretical debates, Section 5 analyzes unique contextual enablers for the US/UK-led initiatives underpinned by operational environments of the war as well as the broader European and transatlantic strategic landscape, leading to a conclusion of the analysis with future implications.

1. Intelligence-led Allied Campaigns to preempt the Russian Moves.

Transatlantic intelligence corporations began with the US-UK bilateral endeavors of collection and analysis of Russia's invasion plan. According to the investigative reporting of the British Broadcasting Corporation

(BBC), a classified source from a Western intelligence agency grasped signs of the invasion planning inside the inner circle of the Kremlin decision-making in the summer of 2021.[4] This early warning kicked off intensive bilateral efforts behind closed doors. Around autumn 2021, the U.S. government confirmed the certainty of Russia's possible invasion scenarios and then took the lead in following intelligence-led security corporations vis-à-vis other NATO members and the broader international audiences.[5] In other words, weaponized disclosure is embedded into a part of the US and UK-led cumulative international responses to preempt Russian moves and defend allies and partners. These intelligence-led allied campaigns can be divided into four key pillars in accordance with the collection targets, granularity, and channels of intelligence sharing, as well as intended effects vis-à-vis target audiences.

The first is "intelligence diplomacy.", which involves sharing classified intelligence products privately with allies and partners to shape common situational awareness and coordinated policy responses. For example, the United States has conducted a series of shuttle diplomacy for classified briefings about possible Russian invasions with other NATO members.[6] Such closed-door intelligence-sharing about Russian malicious behaviors for enabling the coordinated campaign to counter Russian threats has precedents[7] in 2018, namely the international response to the Russian use of a chemical weapon in the UK known as the Salisbury incident as well as the recognition of Russia's violation of the Intermediate-Range Nuclear Forces (INF) Treaty.[8]

The second pillar is the public disclosure of Russian capabilities and intentions about the full-scale invasion. On December 3, 2021, the Washington Post carried the declassified briefing material provided by the US intelligence community, with commercial satellite images highlighting the scale and locations of Russian forces mobilization near the border with Ukraine.[9] Subsequently, the US and the UK relentlessly publicized their analysis and estimate through multiple channels. Their contents (Figure 1) focused on reasonable harbingers which highlighted Russian capabilities (and intentions) for the possible invasion, including the mobilization updates, possible offensive routes, false flag operations in eastern Ukraine, and covert plots against the overthrow of Volodymyr Zelenskyy regime and the installation of Pro-Russian puppet regime. Even after the outbreak of the full-scale war, the US and UK governments have continued their initiatives to transmit the situational awareness of warfighting on the ground to multiple audiences, including the US Department of Defense briefings to journalists and the UK's Defense Intelligence (DI) initiatives to publicize the daily update of their intelligence estimate through social media such as Twitter.[10]

Here, it should be noted that what has been and what's *not* declassified and publicized. Generally, what has been publicized is a finalized analysis instead of a source and methods itself, and major declassifications presented in Figure 1 are not equal in their granularity of evidence to support analysis. The US/UK initiatives are coordinated and nuanced efforts to balance effects by publication and protecting classified sources and methods.[11] In other words, declassified content is the tip of the iceberg compared to the primary information collected and analyzed by the US and the UK, which forms its basis and the intelligence products believed to be shared under the surface with allies in "intelligence diplomacy."[12]

Figure 1: Timeline of the US/UK Weaponize Disclosure from December 2021 to February 24, 2022

Date	Country	Overview of the Declassified Contents
December 3, 2021	US	Leaked briefing material, including satellite images showing the mobilization of Russian military forces near the border with Ukraine and the bases where they were concentrated. It presented the estimate that there have been preparations for a military invasion from multiple fronts on the approximate scale of a maximum of 175,000 personnel, which would be ready by the beginning of 2022 at the earliest.
January 14, 2022	US	The official briefing to the press saying that Russia was deploying operatives to conduct false flag operations in eastern Ukraine to fabricate a pretext for the military invasion of Ukraine. It touched on the evaluation that the false flag operations would be implemented from the middle of January to the middle of February, and the military invasion could start several weeks after that.
January 22, 2022	UK	The official press release about the existence of a covert plot to overthrow the current regime and install a pro-Russian puppet regime. The release exposed the specific names of five Ukrainian nationals, including Yevhen Murayev, a former parliament representative and a candidate for the leadership of the puppet government, noting that the plot was conspired with the Russian intelligence agencies as a part of the Russian invasion planning.
January 28, 2022	US	Multiple leaks from US government officials said that the distribution of emergency medical supplies, such as blood for transfusions, to the mobilized forces along the border had begun, which was unusual for the regular exercise. This analysis could be one of the signs that the mobilization was intended for an actual military invasion instead of the Russian claim of military exercise.
February 3, 2022	US	The official briefing that Russia was creating propaganda images purporting to show massacres of residents in eastern Ukraine. The images themselves have not been publicized, but according to the Department of State spokesperson, the images include equipment falsely proving an attack by Ukrainian armed forces on ethnic Russian residents (e.g., the Turkey-made drone Bayraktar TB2, which is also used by the Ukrainian side), the site of the attack, the dead bodies of the victims and bereaved family members.
February 13, 2022	US	The US National Security Advisor expressed the evaluation that the military invasion by Russia could begin even before the closing of the Beijing Olympics (February 20, 2022).
February 16 - 17, 2022	US/UK	In response to the Russian government's claim of "withdrawal of Russian military forces from the border," both the US and the UK presented the evaluation that the mobilization of Russian military forces along the border was continuing, and they could not confirm any information to verify the

		Russian claim of withdrawal of mobilized forces.
February 23, 2022	US	The U.S. government leaked and let the world news outlets carry the fact that the US had warned the Ukrainian government that the military invasion of the Russian military forces would commence within 48 hours.

(Note) In advance of the US and the UK, in November 2021, the Ministry of Defence of Ukraine[13] released an analysis, including of the scale of the mobilization of Russian military forces along the border and the anticipated invasion routes.

(Source) Prepared by this author based on the officially published information of the governments of the US and the UK and the related media reports.

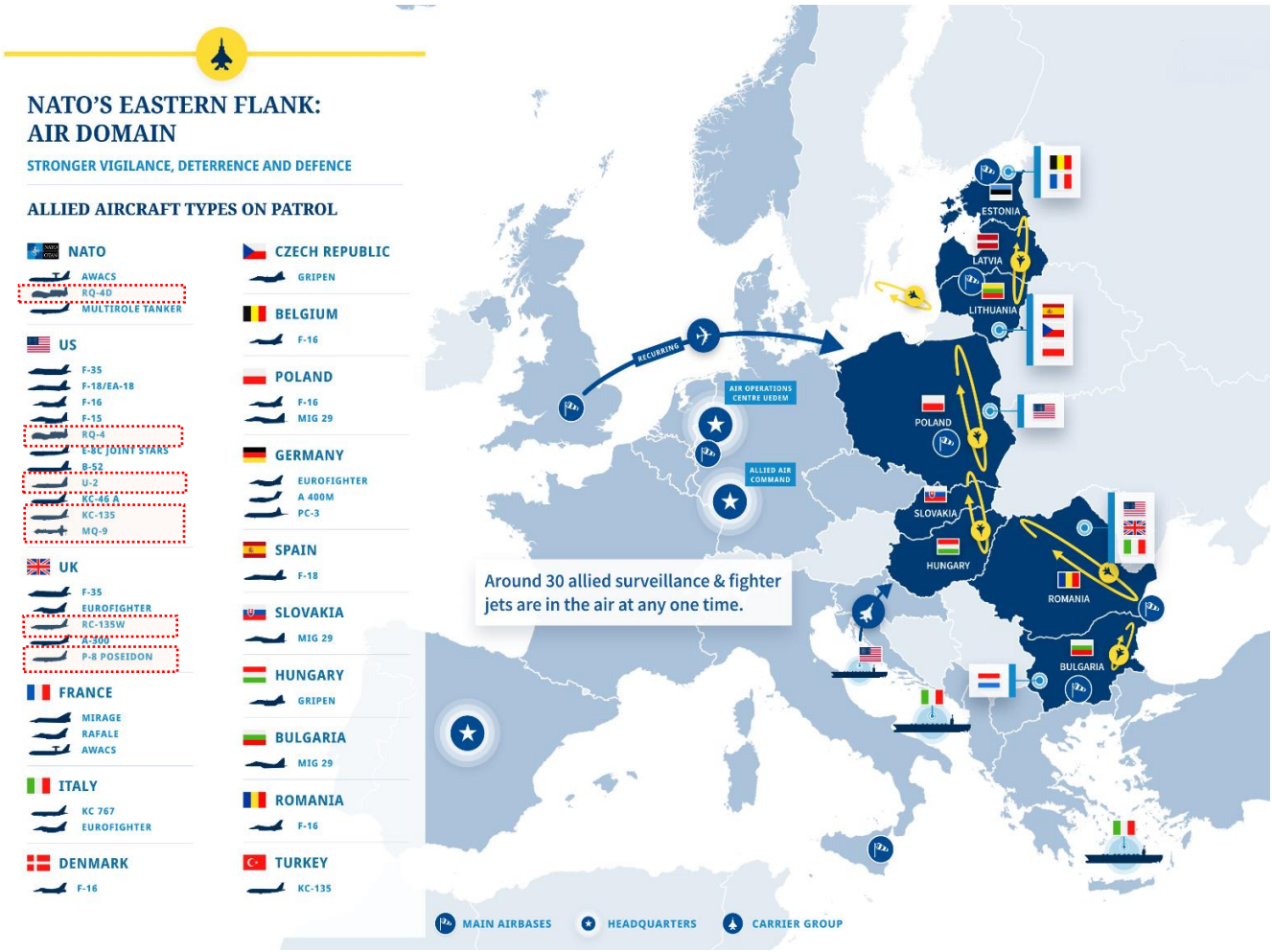
The third dimension is leveraging "cyber threat intelligence (CTI)" for the network defense of public and private entities in Ukraine and the NATO member states. The most notable example is the US-led "hunt forward" missions (hereafter HFM), which deploy the U.S. Cyber Command personnel to the allies and partners (hereafter host-nations) proximate to the U.S. regional competitors to conduct combined network defense and threat-hunting activities with the host-nations.[14] Within each deployment, threat-hunting efforts toward host-nations networks generate insights on technical artifacts as well as behavior tradecrafts of adversary's campaigns, known as "Indicator of Compromise (IoC)," and "Tactics, Techniques, and Procedures (TTPs)," respectively. The IoC/TTPs obtained through HFM have been shared privately in relevant information/intelligence sharing channels for early warning for the network defenders of the U.S. and allies and partners' organizations. In addition, such CTI often has been declassified to be shared with broader audiences outside of the closed information-sharing community. For example, occasional uploads of malware samples to Virus Total and Joint Cybersecurity Advisory, to which USCYBERCOM accelerated their contribution since 2018, represent such government-led disclosure of CTI to scale up outreach to domestic and international industries partners beyond traditional sharing channels.[15]

HFM originated as one of the USCYBERCOM proto-typing initiatives to preempt Russian election interference in 2018, and this root has underpinned its trajectory of development in the following years with its regional priority in the allies and partners in Europe. For the last 5 years since then, HFM has streamlined its operational effectiveness and efficiency through cumulative operational experiences with European host nations, including Ukraine.[16], as it provided the readiness to both USCYBEROM and European host nations through building mutual trust and interoperability.[17] USCYBERCOM, for example, deployed HFM teams to Ukraine in December 2021, and despite its shortened timeline of deployment facing an imminent danger of ground invasion, the team streamlined the process and succeeded in enhancing situational awareness and protection against the Russian threat against Ukraine's critical infrastructures and government networks.[18] The US presence in neighboring NATO member states and readiness in cyberspace have maintained, even after the invasion broke out, to provide CTI-based early warning and network defense support to both Ukraine and the NATO member states.[19]

The fourth pillar is intelligence support to the Ukrainian Armed Forces.[20] The US /UK and the NATO-allied intelligence, surveillance, and reconnaissance (ISR) assets and their forward deployment posture in NATO's eastern flank played important roles (Figure 2).[21] Since late 2021, some investigations have observed the

greater operational track records of the US/UK and NATO's joint aerial ISR assets over Poland and Romania, as well as the sky over the Black Sea.[22] These series of ISR activities contributed to collecting information about the locations of the Russian armed forces.[23] According to media coverages based on leaks, the US has leveraged these collection efforts to formulate finished intelligence products[24] in order to help the air defense and other operations of Ukraine Armed Forces from the outset of the invasion while they officially maintained plausible deniability in their involvements.[25]

Figure 2: Air-based ISR Readiness in the NATO Eastern Flank (As of May 10, 2022)



(Note) ⋯⋯ refers to the US /UK and the NATO-allied aerial ISR assets actively operating from the end of 2021 onwards, either in the NATO Eastern Flank or the Black Sea regions, confirmed with various open-source reporting such as footnotes 20, 22, and 23 of this paper.

(Source) : prepared by this author based on the picture of the NATO Allied Air Command at the following URL; "Allies Stand Together to Bolster NATO's Eastern Flank," NATO HQ Allied Air Command, May 10, 2022, https://ac.nato.int/archive/2022/nato_eAV_air.

One common feature of the four initiatives above is the calculated use of publicity to maximize desired effects vis-à-vis specific target audiences. Despite their differences in the collection targets, granularity,

and channels of sharing, all of them deliberately unveiled their secrecy and tailored levels of visibility toward specific target audiences, including Russia, as well as the allies and partners. While this feature is most notable in weaponized disclosure (the second pillar), others represented the same trait; otherwise, they would have been subject to complete secrecy for their operational security and protection of collection sources and methods.[26] In other words, all initiatives have carefully equated secrecy and publicity of initiatives, calculating respective rationales and tailoring their extents. With this point in mind, the next sections focus on theoretical and practical conundrums over weaponized disclosure in general.

2. Conventional Wisdom on Nation-states Intelligence Disclosure.

Theoretical and practical controversy over weaponized intelligence disclosure starts from and ends with the principle that intelligence is the world of secrecy. Conventional wisdom and practitioner norms suggest that intelligence should not be made public for reasonable concerns. Starting from this point is critical to understand the nature of weaponized intelligence disclosure, enablers, and constraints of the US/UK initiatives in the Russia-Ukraine War context, as well as future implications beyond this war.

The biggest practical concern for nation-state intelligence services is that disclosing intelligence products and activities could jeopardize collection sources and methods. Any disclosure beyond the presentation of conclusions could have certain risks, as a reckless release of analyses allows the surveillance target or a third party to trace back to the sources and methods behind it as the contents and timing of release hint underlying evidence. Even without the target's knowledge of the source and methods, just a suspicion of ongoing collection efforts often triggers the countermeasures by the target, such as hunting moles and changing encryption modes. It can lead to damaging consequences for the future collection capacity of intelligence services[27]. It goes without saying that the loss of sensitive assets could have a detrimental effect on the continuity of future collection and analysis efforts, and if the collection source is human intelligence (HUMINT), the risk is also a matter of life and death.[28] As such, it is natural that intelligence agencies have formed a strong organizational culture against the disclosure of intelligence.[29]

Second, this practical concern also intertwines with theoretical and normative debate over the "core" and "periphery" of intelligence (activities).[30] In essence, the narrower you define what intelligence should be, the stronger the skepticism against weaponized intelligence disclosure becomes. From overt counter-intelligence measures to covert action, theory and history of intelligence tell us that leveraging

intelligence to create visible effects against targets has always been controversial as it may pose risks to revealing one's secret hands and compromising clandestine capabilities.[31] For those who narrowly define the core of intelligence as (secret) collection and analysis to support decision-making or operational support for the future contingency, the initiative is perceived as too risky to legitimize its risks on collection sources and methods in the intelligence-gain/loss equation.[32] Against these backdrops, conventional wisdom has it that nation-state intelligence disclosure results from the politicization of intelligence, implying it is a negative sign eroding intelligence's core mission and code of conduct.[33]

3. Logics and Caveats of Weaponized Disclosure for Intelligence-Effects.

The growing body of academic literature in intelligence studies, however, has challenged the conventional wisdom in Section 2 by presenting empirical case studies of nation-state weaponized disclosure, which cannot be attributed to top-down political considerations and is more motivated by bottom-up national security/counter-intelligence considerations, such as Israeli military and intelligence efforts throughout the 2010s.[34] These findings can provide readers with the theoretical lens to grasp the following logics and caveats behind the US/UK-led weaponized disclosure.

To begin with, previous studies have reached a consensus that a weaponized disclosure could have multiple "target audiences (hereinafter referred to as the "TA")" on which nation-states try to influence and create desired effects through their behavior changes. In other words, a weaponized disclosure could have different ends and means vis-à-vis its TA[35]. It requires a granular understanding of multiple causal mechanisms and assumptions to bridge influence (on audiences) and desired effects without reducing such complexity into catch-all concepts such as "information warfare" and "deterrence by disclosure." With this analytical lens in mind, US/UK-led weaponized disclosure in the Russia-Ukraine War represents the following four possible subsets of the audience-(desired)effects nexus.

The first subset of the audience-effects nexus is the "*disruption*" of adversaries' clandestine/covert campaigns, which its TA includes military/intelligence planners and operatives. Recent studies have theorized that intelligence disclosure could (temporally) disrupt the execution of certain military and intelligence activities if secrecy is indispensable for force protection and mission success. For instance, publicly exposing adversaries' clandestine and covert operations results in subsequent counter-intelligence efforts to burn mission-critical assets and infrastructures, threatening their perception of operational security. These effects can force them to modify their planning and delay ongoing campaigns

because it forces them to rearrange their assets/infrastructures and to take measures to avoid another detection.[36] In addition, repeating the failure of operational security reduces decision-makers trust in the competence of their military/intelligence apparatus while it also induces paranoia in traitors among operational planners. Such psychological effects also cause friction in operational planning as they force planners to modify their ways of communication and increase cumulative costs and risks, leading to a greater chance of mission failure.[37]

The second audience-effects nexus is the *"sense/meaning-making"*[38] for policy-makers and public opinions in third countries, including allies, partners, and swing-states between adversaries' efforts. Preventive public exposure to adversaries' malicious behaviors reduces uncertainty on situational awareness while it also underpins dominant narratives in information space with a first-mover advantage, which influences TA's perceptions and behavior patterns. These effects help to shape favorable international agendas to legitimize and convene collective policy responses and mitigate the negative consequences of adversarial information maneuvers. The UK's initiatives, called "prebuttal," follow the same logic by preemptively exposing and refuting Russian disinformation before establishing its dominance in the global information space.[39]

A logical question arises as to "*why nation-state intelligence disclosure matters"* about the sense/meaning-making effects. Specifically, "*Is there a difference between (a) publicizing contents as a form of declassification of nation-state intelligence and (b) open-source reporting by private sectors/civil society, provided that the publicized contents themselves are the same*?" Recent studies have suggested that the answer is "yes.", elaborating the unique strength of nation-states' disclosure to a unique dynamic of the 21st century's information environment.

A strength of the nation-state's public disclosure of intelligence is "*augmented attention*" vis-à-vis attention economy dynamics in the highly contested information sphere. Ofek Riemer points out that gaining TA's attention to published content becomes more and more challenging with the exponential growth of volumes and speed of information flow, accelerated by the proliferation of ICT and the emergence of social media. Losing their traditional privilege, governments today have been competing with various private entities and individuals to win and retain the audience's attention to the information they try to disseminate. In this highly contested information environment, the declassification of intelligence is a catalyst to induce outstanding attention, leveraging the exceptionalness of revealing government secrets and the public trust in the intelligence agencies' analytical competence in national security affairs.[40]

This augmented attention by nation-states could catalyze and accelerate the following two dynamics of the information ecosystem. First is the *"knowledge co-production"*[41] or "*reciprocal investigative relationship and parallel evidencing*"[42] between the public and private sectors. In some cases, the government declassification of analysis provides initial insights into targets with investigators in private sectors/civil society. This triggers their follow-up investigations and additional qualitative and quantitative information flow by their respective collection coverages. Such tacit feedback from private sectors and civil society efforts can benefit the government because it increases overall situational awareness of society and could alleviate intelligence-gain loss calculations of government sources in the long run.[43]

The second dynamic is the "*social construction of trustworthiness (through third-party verification),*" which can be reinforced as a byproduct of the first dynamic. For example, the survey experiments and policy analysis by Erik Lin-Greenberg and Theo Milonopoulos suggest that private sector/ civil society verification of the government claims, utilizing commercial satellites, enhances the trustworthiness of the analyses and encourages stronger public support for the claims of the government.[44] This third-party verification and trust construction dynamics could alleviate the problems of untrustworthiness of weaponized disclosure by nation-states' intelligence apparatus (see the following Section 4).

How can we assess the effectiveness and efficiency of the US/UK initiatives vis-à-vis these theoretical frameworks of weaponized disclosure? Firstly, the disclosure of substantial Russian covert/clandestine action plots, such as the puppet regime installation, has disrupted Russia's hybrid conflict strategy to achieve fait accompli and seize the escalation dominance without triggering the Ukraine military resistance and third-party support in the case of the annexation of the Crimea. The unprecedented scale/speed of US/UK initiatives from the end of 2021 has kept the attention of the world on the Ukraine situation, helping to shape the perception of an imminent and substantial risk of Russian invasion and the lack of legitimacy of the actions of Russia, which shaped baseline of the following international political, economic, and military supports to Ukraine.[45] In tandem with Kyiv's initial military success, US/UK initiatives have disrupted Russia's original Blitzkrieg and cumulatively increased their costs of waging a war of attrition.

Second, weaponized disclosure in this war proves that "knowledge co-production" and "social construction of trustworthiness" dynamics have been amplified by an emerging open-source intelligence (OSINT) community practice. US/UK disclosure in December 2021 triggered the following open-source investigations by the research institutions and Russian/military experts, supplementing the validity of the

US/UK analysis. Despite the controversy on the ill-standardization of practices of the OSINT community, rapid investigations/verification processes vis-à-vis government disclosure have prevented Russian disinformation and narrative from taking its dominance in the global information sphere.[46]

Third is a caveat of weaponized disclosure. It did not and will never be able to "deter." resolved adversaries from overt and full-scale armed conflicts, despite policy-community narratives of "deterrence.". Even if weaponized disclosure as a "disruption" could dissuade the adversarial actions, the logic is closer to the intelligence vs counterintelligence contests below the threshold of armed conflicts with both sides having an incentive to de-escalate, rather than the logic of warfighting and coercion leveraging the power to hurts and risk of escalation. The effectiveness of weaponized disclosure relies on the implicit assumption that revealing adversaries' covert/clandestine activities could limit the intensity and frequency of future activities, as those exposed perceive the risks and incentive to keep restraints on their maneuvers for political escalation and operational security considerations.[47]

Against these backdrops, it is not likely to change the behaviors of adversaries when they do not care about the consequences, and/or the exposure could constitute the desired effects to their target audiences[48]. It is not able to change the course of resolved actors, who are willing to escalate the situation from the gray zone to high-intensity conflicts supported by the overt use of the armed forces.[49]

4. Disclosure Dilemma vis-à-vis Vicious Cycle of Trust Erosion.

The biggest challenge of weaponized disclosure, as touched on in Section 2, is managing the "disclosure dilemma," which require policymakers to calculate equity between creating military/policy effects for utilizing intelligence and protecting source and methods for future collection and analysis. This intelligence-gain/loss equation is not isolated within weaponized disclosure itself, but it can be intertwined with the broader implications of prioritization, resource allocation, and organizational-cultural preferences of intelligence activities. For example, Jake Harrington warns that reckless disclosure could incentivize intelligence services to be reluctant to share the analysis from classified sources as they perceive risks of politicized handling of products without considering the protection of sources and methods. Leveraging intelligence (disclosure) as a policy means requires an institutionalized equity process with reasonable concerns from the intelligence apparatus in the loop. [50]

That is easy to say but difficult to do. In practice, striking a balance between the desired effects of TA and keeping secrecy for future collection efforts has been very challenging for the following reasons. First, intelligence-gain loss judgment takes time and costs. Rationales for protecting sources and methods tend to justify the overclassification and make timely and scalable disclosure for the intended effects impossible. Second, keeping the quality and quantity of the disclosure is difficult due to the limited available resources. In some cases, governments may face no choice but to rush out the release of the finalized products without substantial evidence and analytical rigor. In this setting, the trustworthiness of the declassified analysis would only be guaranteed by inter-subjective trust, constructed from the TA's perceptions of the intelligence agencies' historical (in)competence.[51]

Finally, the more prolonged and repeated it becomes, the greater the risks to fall into a vicious circle of eroding trust and diminishing effects as it leads to the decline in augmented attention and perceived trustworthiness from the TA. As noted above, pursuing scale/scope of disclosure and protection of classified sources simultaneously would force intelligence agencies to give up transparency and quality of the publicized products. However, publicizing untransparent and unverified analysis is vulnerable to the adversaries' information/narrative manipulation to damage the trustworthiness of the claims, whether the publicized analysis represents material(scientific) truth or not. Once the trust from TA has been damaged, and the bonus of the initial attention is likely to diminish like the fable of the "boy who cried wolf, it becomes extremely difficult to maintain the desired effects for a longer timeframe.[52]

5. Enablers in the Russia-Ukraine War and Transatlantic Security Landscape?

The challenges of the disclosure dilemma and vicious cycle of trust erosion is structural and have frequently appeared in the historical precedents, for example, collective public attribution to malicious cyber campaigns since 2017.[53] In this sense, the necessary question is, "*What has alleviated the US/UK dilemma in the context of the Russia-Ukraine War, which can serve as enablers for unprecedented scale and speeds of the initiatives?*" Answering this question, it is worth highlighting the following four factors vis-à-vis geopolitical contests of the transatlantic security landscape.

One of the biggest enablers is the characteristic of the Russia-Ukraine War and its operational environment, which has shaped the nature of the collection coverage and information environments leveraged for weaponized disclosure. To begin with, the massive scale mobilization, logistics, and sustainment efforts of the Russian Armed Forces around the Ukraine border and in Belarus since 2021

are quite extraordinary. It is difficult to conceal and cannot be reasonably accounted for the Russian claims of the military exercise. In this setting, public disclosure of their mobilization and readiness around the border could allow military and intelligence experts to follow their heuristic analytical process for inferring the worst-case possibility of the Russian invasion in reference to material capabilities despite the uncertainty of the Kremlin's true intentions.[54]

The US/UK's declassification of the intelligence has exploited these material and inter-subjective attributes of the large-scale land warfare modality. Gaining insights from highly sensitive and unpublicizable collection coverage from their own sources as well as allies and partners, both countries have leveraged low-sensitive sources, namely commercial satellite imagery and publicly available social media data feeds about the Russian mobilization and maneuvers, to create the effects through declassification[55]. For example, the U.S. declassification of satellite imagery in December 2021 was not sensitive as its sources have been commoditized with the growth of commercial satellite service providers.

Second, and supported by the first point, the US/UK-led weaponized disclosure have been able to accelerate and leverage the chains of effects of knowledge co-production / reciprocal investigative relationship and parallel evidencing (see Section 3). Even a risk-controlled disclosure enabled by publicly available sources has sufficient effects to expose critical geographical nodes of the Russian mobilization and send a publicly available cue for the follow-up open-source investigation efforts by private/civil society players worldwide, including academics, think-tankers, and OSINT practitioners, which resulted in a reduction of source and methods compromise as the exponential flow of open-source data and analytic insights could provide a plausible cover for the government's sensitive sources and methods and supported the trustworthiness of the analyses.[56]

Third, the US/UK organizational learning vis-à-vis their experience has been critical because the weaponized disclosure requires shared commitments for institutionalizing the process from policymakers and intelligence services, given the latter's reluctance (See Section 4). For instance, the US intelligence community has surged declassification experts and concentrated additional resources to accomplish the accelerated intelligence-gain loss equity and maintain the quality of the analyses in response to the White House policy direction.[57] Such an extraordinary response relies on shared commitments among policymakers and intelligence agencies about the ends and means of the weaponized disclosure.[58] The US and UK have been shaping their learning and adaptation from (failure of) responses to the annexation of Crimea by Russia in 2014 and Russia's interference in the US presidential election in 2016.[59]

Finally, the cumulative outcomes of the transatlantic security corporation for countering Russian hybrid threats have ensured the readiness of the US/UK's weaponized disclosure. NATO and EU member states have developed their collective deterrence and resilience posture against hybrid threats since 2014, as a full spectrum of threats, from Russian nuclear/conventional forces to covert political interference against democracy, has been challenging them. Over 8 years of cumulative national and regional efforts have strengthened early-warning capacity from the allied ISR/cyber units and interoperability of the intelligence-driven allied campaigns within member states and beyond, namely intelligence-sharing with Ukraine.[60] The fruits have also eased the challenges of the disclosure dilemma as it allows diversifications of available sources and coordinated diplomatic supports to supplement the trustworthiness of the analysis both through back-channel and public.[61]

In sum, the US/UK intelligence-driven allied campaigns, including weaponized disclosure in the Russia-Ukraine War, are not in a vacuum from a strategic depth of time and space. It has been predicated on the collective inheritances from the transatlantic regional security corporation vis-à-vis the resurgence of belligerent Russia in the era of great power competition.

6. Conclusion.

Bridging theoretical insights and empirical analysis of the Russia-Ukraine War's dynamics, this NIDS commentary concludes that the US/UK weaponized disclosure is not a vacuum in the sense that it poses challenges of disclosure dilemma to the intelligence services, and its effectiveness/efficiency is always context-dependent underpinned by their TA and strategic as well as operational environments. As such, it is worth highlighting the necessity of nuanced analysis and further discussion about the prospects of weaponized disclosure in specific dimensional and regional settings instead of underestimating the caveats of the initiative as depicting it as a silver bullet of information warfare.

For example, there has been consensus that the utility of the US/UK weaponized disclosure before the full-scale invasion should be assessed vis-à-vis limitations of the viable ends and means. That is, the US/UK's ruling out the options of direct armed conflict and escalation vis-à-vis Russia defined their viable theory of victory as disrupting Russia's military fait accompli by supporting the Ukraine resistance and dragging Russia into the protracted war under strong international pressure, instead of deterring full-scale invasion itself. In this sense, the US/UK weaponized disclosure has served its achievable goals.[62] Beyond the case of the Russia-Ukraine War, armed conflicts underpinned by different operational

environments could shape the weaponized disclosure in different modalities vis-à-vis its strategic goals.[63] In this sense, future planning efforts also require an assessment of enablers and constraints for the weaponized disclosure of possible regional contingency beyond Europe, namely the Indo-Pacific and the Middle East.

The author, however, also concludes that a generalizable and more substantial implication of the US/UK weaponized disclosure is having scholars and practitioners revisit the fundamental question of intelligence studies: "*What intelligence means and what it should do and be like*."

This final point appears in the following two senses. First, the weaponized disclosure in the Russia-Ukraine War showed us dynamic knowledge/trust co-production dynamics between the government and stakeholders outside the traditional intelligence cycle, underpinned by the growth of private-sector cyber threat intelligence industries and civil-society-based OSINT community.[64] To be fair, the essentiality of secret intelligence remains constant, and secrecy will likely be an enduring philosophy of the nation-state intelligence apparatus[65]. At the same time, contemporary national security challenges such as counterterrorism and cyber security in collaboration with non-government stakeholders have required Western intelligence services to adopt their roles and organizational culture, balancing between (1) secretive nature as intelligence apparatus for the customers of the traditional intelligence cycle, and (2) public-facing functions for intelligence-enabled homeland security.[66] The US/UK moves in the Russia-Ukraine War, in this sense, represent the latest example of the continuous adaptation process of intelligence services[67] vis-à-vis the dynamic security landscape underpinned by contested information environments in the 21st century.[68]

Second, the disclosure dilemma of the weaponized disclosure also reminds us of the recurring debate of the "core" and "periphery" of intelligence. Conventional academic wisdom has maintained differentiation between a narrower sense of "intelligence (collection and analysis)" and "actions (for effects)," and strong professional norms of the Western intelligence apparatus have taken it for granted that intelligence apparatus is and should be prioritizing collection and analysis over action. However, growing academic debate on covert actions and special operations has told us there have always been blurred lines between "intelligence" and "direct action," national or organizational preference among various types of intelligence activities has been historically neither self-evident nor universal.[69]

In conclusion, the discussion of weaponized disclosure requires both scholars and practitioners to be mindful of the following. questions: "*what does intelligence mean in their national context, and what*

national intelligence apparatus has been responsible for." as well as "*whether and how weaponized disclosure, categorized as a form of intelligence-enabled effects functions like covert action, could be reconciled with their existing understanding, practices, and organizational culture of intelligence.*"

[End]

1 This term traditionally refers to the following four meanings: (a) government intelligence apparatus and their community (the intelligence community), (b) the missions and activities of (a), (c) the final products of the information collection and analyses, which are a part of (b), and (d) the process of producing and disseminating the products, commonly known as the intelligence cycle. This paper also uses either term, mainly focusing on the government's initiatives. Furthermore, the author differentiates (c) (finalized intelligence products) and "classified information (obtained through secretive sources and methods)" as the former often consists of publicly available information, though the product is generally classified as well. See the followings. 川上高司、樋口敬祐、上田篤盛、志田淳二郎『インテリジェンス用語辞典』（並木書房、2022 年）91-93 頁。（Takashi Kawakami, Keisuke Higuchi, Atsumori Ueda, and Junjiro Shida, *Dictionary of Intelligence Studies* [Namiki Shobo, 2022] 91-93.）；小林良樹『なぜ、インテリジェンスは必要なのか』（慶應義塾大学出版会、2021 年）16-18 頁。（Yoshiki Kobayashi, *Essentials of Intelligence* [Keio University Press, 2021] 16-18.）

2 See the following. Ministry of Defense, *Defense of Japan 2023*, the annual white paper of Japan's Ministry of Defense, September 4, 2023, pp. 239, 241, 341-345. https://www.mod.go.jp/en/publ/w_paper/wp2023/DOJ2023_EN_Full.pdf; "Integrated Information Warfare with Special Regard to the Cognitive Dimension," Ministry of Defense, https://www.mod.go.jp/en/d_architecture/infowarfare/index.html (last accessed October 26, 2023).

3 Regarding the disclosure dilemma and its relationship with intelligence disclosure, see the following. Huw Dylan and Thomas J. Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," *Survival* 64, no. 4 (July 4, 2022): 51–54; Allison Carnegie and Austin Carson, *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*, 1st ed. (Cambridge: Cambridge University Press, 2020), 28–39.

4 Gordon Corera, "Ukraine: Inside the Spies' Attempts to Stop the War," *BBC News*, April 8, 2022, https://www.bbc.com/news/world-europe-61044063.

5 Ibid.; Ellen Nakashima and Ashley Parker, "Inside the White House Preparations for a Russian Invasion," *The Washington Post*, February 14, 2022, https://www.washingtonpost.com/national-security/2022/02/14/white-house-prepares-russian-invasion/.

6 Corera, "Ukraine: Inside the Spies' Attempts to Stop the War"; Julian E. Barnes, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion," *The New York Times*, February 3, 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html.

7 Barnes, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion."

8 Refer to the following regarding this point. The Intelligence and Security Committee of Parliament (ISC) "Intelligence and Security Committee of Parliament: Russia," HC 632, July 21, 2020, 37-39, https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.; ；鶴岡路人「ポスト INF 条約の NATO と欧州安全保障」 日本国際問題研究所編『混迷する欧州と国際秩序』（平成 30 年度外務省外交・安全保障調査研究事業、2019 年 3 月）100-101 頁。（Michito Tsuruoka, "NATO and European Security in Post-INF Treaty Period" in *Europe in Turbulence and the International Order* edited by The Japan Institute of International Affairs [FY2018 Ministry of Foreign Affairs of

Japan Foreign/Security Affairs Research Project, March 2019] 100-101.）

9 Shane Harris and Paul Sonne, "Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns," *The Washington Post*, December 3, 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

10 Karla Adam, "How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine," *The Washington Post*, April 22, 2022, https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/.

11 Ken Dilanian et al., "The U.S. Is Using Declassified Intel to Fight an Info War with Russia, Even When the Intel Isn't Rock Solid," *NBC News*, April 6, 2022, https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014.

12 Adam, "How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine."

13 Howard Altman, "Russia Preparing to Attack Ukraine by Late January: Ukraine Defense Intelligence Agency Chief," *Military Times*, November 20, 2021, https://www.militarytimes.com/flashpoints/2021/11/20/russia-preparing-to-attack-ukraine-by-late-january-ukraine-defense-intelligence-agency-chief/.

14 HFM is a combined "threat-hunting" activities by Cyber Command and the host countries. With regard to threat-hunting activities and CTI, see the following. 石川朝久『脅威インテリジェンスの教科書』（技術評論社、2022 年）2-172 頁。
（Tomohisa Ishikawa, *Cyber Threat Intelligence,* [Gijutsu-Hyoron Co., Ltd., 2022] 2-172.）

15 About HFM's concepts of operations and their geographical scope, see the following. Timothy D. Haugh et al., "Agile Collaboration in Defense of the Nation," in *Ten Years In: Implementing Strategic Approaches to Cyberspace*, ed. Schneider, Jacquelyn G., Goldman, Emily O., Warner, Michael, Newport Papers (Newport, Rhode Island: Naval War College Press, 2020), 97–108; Julian E. Barnes, "U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China," *The New York Times*, November 2, 2020, Online edition, https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html. ; Michael Warner, *US Cyber Command's First Decade*, Aegis Series Paper 2008 (Washington, DC: Hoover Institution/Stanford University, 2020), 18–21; The National Security Agency, "2021 NSA Cybersecurity Year in Review" (Fort Meade, Maryland, February 3, 2022), 3–4, 6, 10,

https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_Cybersecurity_Year_in_Review_20220203.PDF.

16 Sean Lyngaas, "Cyber Command's Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia," *CyberScoop*, March 14, 2019, https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.

17 Martin Matishak, "One-on-One with the Air Force's Cyber Chief," *Recorded Future*, April 18, 2022, https://therecord.media/one-on-one-with-the-air-forces-cyber-chief/.

[18] Dina Temple-Raston, "Q&A with Gen. Hartman: 'There Are Always Hunt Forward Teams Deployed,'" *Recorded Future*, June 20, 2023, https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here.

19 Based on the testimony of U.S. Cyber Command Commander and National Security Agency Director Paul M. Nakasone in the United States Senate Committee on Armed Services on April 5, 2022. Refer to the following. *Posture Statement of General Paul M. Nakasone Commander, U.S. Cyber Command Before the 117th Congress Senate Committee on Armed Services,* 117th Cong. (2021) (General Paul M. Nakasone, Commander, U.S. Cyber Command) 3. ; The United States Cyber Command, "U.S. Conducts First Hunt Forward Operation in Lithuania," U.S. Cyber Command, May 4, 2022,

https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/.

20 An anonymous U.S. military intelligence officer mentioned that the forward deployment of ISR assets on the eastern flank of the allies, such as Poland and Romania, has been reinforced until about February 2022, in the shade of the reassurance package vis-à-vis the member states. See the following. Ken Klippenstein and Sara Sirota, "U.S. Quietly Assists Ukraine With Intelligence, Avoiding Direct Confrontation With Russia," *The Intercept*, March 17, 2022, https://theintercept.com/2022/03/17/us-intelligence-ukraine-russia/.

21 Ibid. See the following references about the forward deployment of the conventional military forces in NATO's eastern flank and the background to strengthening that posture from 2014 onwards. 合六強「3 つの'ショック'に揺れる NATO」日本国際問題研究所編『混迷する欧州と国際秩序』（令和元年度外務省外交・安全保障調査研究事業、2020 年 3 月）99-110 頁。（Tsuyoshi Goroku, "NATO Shaken by Three 'Shocks'" in "Europe in Turbulence and the International Order" edited by The Japan Institute of International Affairs [FY2019 Ministry of Foreign Affairs of Japan Foreign/Security Affairs Research Project, March 2020] 99-110.）

22 The operating status of aerial ISR assets over the NATO allies surrounding Ukraine and the Black Sea have been tracked and visualized, to some extent, through open-source investigations by OSINT experts utilizing Flightradar24 and other sources. See the following. Thomas Newdick, "This Is The Armada Of Spy Planes Tracking Russia's Forces Surrounding Ukraine," *The Drive*, February 18, 2022, https://www.thedrive.com/the-war-zone/44337/these-are-the-planes-keeping-watch-on-russian-forces-around-ukraine.

23 Kieran Devine, "Russia-Ukraine Crisis: What Are NATO Spy Planes Doing to Keep Tabs on the Russians?," *Sky News*, February 8, 2022, https://news.sky.com/story/russia-ukraine-crisis-what-are-nato-spy-planes-doing-to-keep-tabs-on-the-russians-12536567.

24 Larisa Brown, "How Western Spy Planes Keep Tabs on Russian Tactics," *The Times*, March 11, 2022, https://www.thetimes.co.uk/article/how-western-spy-planes-keep-tabs-on-russian-tactics-8slcm0j22.

25 Among the administration officials and members of Congress, there has been a concern about the possibility that it would be seen as a direct military engagement with Russia due to the provision of the ISR for tactical targeting purposes. This concern has allegedly limited the granularity and speed of intelligence sharing from the US government to the Ukraine Armed Forces from the outbreak of the war, and declaratory policy about this initiative has changed several times. See the following. Ken Dilanian et al., "U.S. Intel Helped Ukraine Protect Air Defenses, Shoot down Russian Plane Carrying Hundreds of Troops," *NBC News*, April 26, 2022, https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-protect-air-defenses-shoot-russian-plane-carry-rcna26015.

26 See the following for the logic behind publicizing ISR activities for signaling purposes. Thomas G. Mahnken and Grace B. Kim, "Deterrence by Detection: Using Surveillance to Pre-Empt Opportunistic Aggression," *NDC Policy Brief* (Rome,: NATO Defense College, January 14, 2021), 2–4; Erica D. Borghard, "U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace," *NetPolitics* (blog) (New York: Council on Foreign Relations, April 22, 2020), https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace.

27 See the following. Carnegie and Carson, *Secrets in Global Governance*, 28–39.

28 Ofek Riemer and Daniel Sobelman, "Coercive Disclosure: Israel's Weaponization of Intelligence," *War on the Rocks*, August 30, 2019, https://warontherocks.com/2019/08/coercive-disclosure-israels-weaponization-of-intelligence/; Douglas London, "To Reveal, Or Not to Reveal: The Calculus Behind U.S. Intelligence Disclosures," *Foreign Affairs*, February 23, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-02-15/reveal-or-not-reveal.

29 Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale

Intelligence Problem," *Intelligence & National Security* 36, no. 2 (February 23, 2021): 269–71; Carnegie and Carson, *Secrets in Global Governance*, 31.

[30] Mark Stout and Michael Warner, "Intelligence Is as Intelligence Does," *Intelligence & National Security* 33, no. 4 (June 7, 2018): 517–26.

31 Carnegie and Carson, *Secrets in Global Governance*, 6–8, 26–33; Lindsay, "Cyber Conflict vs. Cyber Command," 261; Timo Steffens, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage* (Wiesbaden, Germany: Springer Vieweg, 2020), 174.

32 Riemer and Sobelman, "Coercive Disclosure: Israel's Weaponization of Intelligence"; London, "To Reveal, Or Not to Reveal."

[33] Ofek Riemer, "Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States," *Contemporary Security Policy* 42, no. 4 (October 2, 2021): 554–83.

34. Ibid.

[35] About multiplicity of target audiences, see the following. Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," Journal of Strategic Studies, Published online (March 2021), 5–8, https://doi.org/10.1080/01402390.2021.1895117; Steffens, Attribution, pp. 173–180. ；瀬戸 崇志「パブリックアトリビューションの'拡散'と'多様化' ——政策当局間の'多様化'の国際比較研究——」『安全保障戦略研究』、第 3 巻 2 号（2023 年 3 月）, 69-70 頁。（Takashi SETO, "Diffusion and Diversification in Public Attribution Policies of Cyber Operations: Comparative Attribution Politics in the US Instrumentation and EU Judicialization," *Security and Strategy*, 3, no.2, [March 2023] 69-70.）

36 Ibid., 556–59, 566–70; Ofek Riemer, "Intelligence and the War in Ukraine: The Limited Power of Public Disclosure," *INSS Insights* (Tel Aviv: The Institute for National Security Studies, March 27, 2022), 6, https://www.inss.org.il/wp-content/uploads/2022/03/no.-1577.pdf; Matthew Armelli et al., *Named but Hardly Shamed: The Impact of Information Disclosures on APT Operations*, SIPA Capstone Project 2020 (Washington, DC: Columbia University's School of International and Public Affairs[SIPA], 2020), iii, 92-95; "Russian Spooks Are Being Kicked out of Europe En Masse," *The Economist*, April 7, 2022, https://www.economist.com/europe/2022/04/07/russian-spooks-are-being-kicked-out-of-europe-en-masse.

37 Riemer, "Intelligence and the War in Ukraine," 4–5; J. D. Work, "Successful Counter-Cyber Operations Secure US Election," *Janes Intelligence Review* (Jane's Group UK Limited, January 28, 2021), 6.

[38] See the following about the concept of sense-making/meaning-making. Florian J. Egloff, "Public Attribution of Cyber Intrusions," *Journal of Cybersecurity* 6, no. 1 (September 14, 2020): 1–12.

39 Dan Lomas, "To Brief, Or Not to Brief: UK Intelligence and Public Disclosure," RUSI Commentary (London: Royal United Services Institute, February 2, 2022), https://rusi.org/explore-our-research/publications/commentary/brief-or-not-brief-uk-intelligence-and-public-disclosure.

40 Riemer, "Politics Is Not Everything," 557, 562–66.

[41] Karen Lund Petersen, "Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?," *Intelligence & National Security* 34, no. 3 (April 16, 2019): 322–24.

[42] Ardil Janjeva, Alexander Harris, and Joe Byrne, *The Future of Open Source Intelligence for UK National Security*, RUSI Occasional Paper (Royal United Services Institute for Defence and Security Studies, Alan Turing Institute's Centre for Emerging Technology and Security, 2022)., vii-ix, 12-14.

43 Petersen, "Three Concepts of Intelligence Communication," 322–24; Janjeva, Harris, and Byrne, *The Future of Open Source Intelligence,* 12-14.

44 Erik Lin-Greenberg and Theo Milonopoulos, "Private Eyes in the Sky: Emerging Technology and the Political Consequences of Eroding Government Secrecy," *The Journal of Conflict Resolution* 65, no. 6 (February 8, 2021): 6-8. 22-24.

45 Dan Lomas, "Weaponizing Truth： UK Intelligence Public Information and Ukraine," *In-Depth Briefing* (Surrey: The Centre for Historical Analysis and Conflict Research[CHACR], April 22, 2022), 5; Riemer, "Intelligence and the War in Ukraine," 3–4; London, "To Reveal, Or Not to Reveal."

46 Lomas, "Weaponizing Truth," 3–4; London, "To Reveal, Or Not to Reveal."

47 See the following about the mechanism of "disruption" in the context of counterintelligence. Hank Prunckun, *Counterintelligence Theory and Practice* (London, United Kingdom : Rowman & Littlefield, 2019), 223–25; Jon Bateman, "The Purposes of U.S. Government Public Cyber Attribution," in *Managing U.S.-China Tensions Over Public Cyber Attribution*, ed. Ariel E. Levite et al. (Washington, D.C: Carnegie Endowment for International Peace, 2022), 14–24; Jason Healey, Neil Jenkins, and J. D. Work, "Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations," in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2020), 255–57.

48 Recent scholarly works and practitioners' analyses have pointed out that Russian ways of covert action, known as "active measures." aim to spread fear and division in their targets through implausible deniability of their presence, whether in physical space or cyberspace, so there is a risk that the exposure by defenders would have an adverse effect because it could be beneficial to their strategic calculus. See the following. Chris Cruden and Nicholas Krohley, "Flunking the New York Times Test: Making Sense of Russian 'Covert' Action," *Modern War Institute* (blog), February 21, 2022, https://mwi.usma.edu/flunking-the-new-york-times-test-making-sense-of-russian-covert-action/; Rory Cormac, Calder Walton, and Damien Van Puyvelde, "What Constitutes Successful Covert Action? Evaluating Unacknowledged Interventionism in Foreign Affairs," *Review of International Studies* 48, no. 1 (May 24, 2022): 112–13, 126–27. 佐々木 勇人「ロシアを背景とするサイバー攻撃グループによるサボタージュ目的/偽情報作戦としての攻撃活動とその対策について」 『CISTEC journal』第 198 号（2022 年 3 月）68 頁。（Hayato Sasaki, "Characteristics and Countermeasure of Russian-Threat actors Cyber Sabotage and Disinformation Campaigns," *CISTEC Journal* No. 198 [March 2022] 68.）

49 Riemer, "Intelligence and the War in Ukraine," 4; Lomas, "Weaponizing Truth," 5; Riemer and Sobelman, "Coercive Disclosure: Israel's Weaponization of Intelligence."

50 Jake Harrington, "Intelligence Disclosures in the Ukraine Crisis and Beyond," *War on the Rocks*, March 1, 2022, https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/.

51 See the following about the erosion in the trustworthiness of the analyses due to lack of transparency on supporting evidence. Carnegie and Carson, *Secrets in Global Governance*, 37–39.

52 See the following about the possibility of the vicious cycle. Harrington, "Intelligence Disclosures in the Ukraine"; Amy Zegart, "The Weapon the West Used Against Putin," *The Atlantic*, March 5, 2022, https://www.theatlantic.com/ideas/archive/2022/03/russia-ukraine-invasion-classified-intelligence/626557/.

53 See the following. Steffens, *Attribution* , 175–76; William Hoverd, "Cyber Threat Attribution, Trust and Confidence, and the Contestability of National Security Policy," in *Emerging Technologies and International Security*, ed. Steff, Reuben Burton, Joe Soare, Simona R. (London : Routledge, 2020), 221–39; Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 55–81.

54 For example, the United States presented an analysis that is hard to imagine other than preparations for a military invasion, namely the distribution of emergency medical supplies, persuasively showing that Russia intended to launch a military invasion. However, it is reported that the evaluation of the intentions of the Russian side was not necessarily monolithic among the NATO members from the beginning, and even in the process of "intelligence diplomacy," in particular aligning the situation evaluations of the US and the UK with those of Germany and France was extremely heavy going. See the following about points above. Neveen Shaaban Abdalla et al., "Intelligence and the War in Ukraine: Part 1," *War on the Rocks*, May 11, 2022, https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/.

55 See the following about the role of the information provided by the Ukrainian government and residents before and after the military invasion and the role of commercially and publicly available information sources, including commercial satellite images. Ibid.; Peter Aldhous and Christopher Miller, "How Open-Source Intelligence is Helping Clear the Fog of War in Ukraine," BuzzFeed News, March 3, 2022, https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social.

56 Lomas, "Weaponizing Truth," 4; Chris Taylor, "Presenting Intelligence: From Iraq WMD to the New Era of 'Strategic Downgrades,'" *The Strategist*, August 13, 2023, https://www.aspistrategist.org.au/presenting-intelligence-from-iraq-wmd-to-the-new-era-of-strategic-downgrades/.; Lomas, "Weaponizing Truth," 4; "Expert Views on the War in Ukraine," *King's Intelligence and Security Group Blogposts* (blog), April 21, 2022, https://kisg.co.uk/blogposts/f/expert-views-on-the-war-in-ukraine.

57 Corera, "Ukraine: Inside the Spies' Attempts to Stop the War."

58 Harrington, "Intelligence Disclosures in the Ukraine."

59 About the organizational learning and adaptation process in recent years among the US and UK's military and intelligence apparatus, see the following. Besty Woodruff Swan and Bryan Bender, "Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders," *POLITICO*, April 26, 2021, https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723; Adam, "How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine."

60 About collective readiness against Russian hybrid threats, See the following. Peter Poptchev, "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages," *Information & Security An International Journal* 45 (2020): 35–55. 志田淳二郎『ハイブリッド戦争の時代―狙われる民主主義』（並木書房、2021 年）42-44, 151- 170 頁。（Junjiro Shida, "Hybrid War: Enduring Threats to Democracy" [Namiki Shobo, 2021] 42-44, 151-170.）

61 Refer to the following references, respectively, for the problem of evaluation sharing through the "intelligence diplomacy" among NATO members in the process up until the military invasion this time and the development in NATO members of the response in the intelligence release policy with respect to the hybrid threat in the second half of the 2010s. Lomas, "Weaponizing Truth," 4–5; Poptchev, "NATO-EU Cooperation in Cybersecurity and Cyber Defence ," 42–45.

62 As already stated in the main text, in the first place it can be concluded that "deterrence of military invasion by the armed forces" is an unachievable goal in the weaponized disclosure. Riemer has pointed out that, supposing direct military intervention by the US/UK armed forces could be imagined, there is a possibility that a different response may have been found reasonable due to demands for the preservation of sources and methods of support for the military operations themselves. See the following. Riemer, "Intelligence and the War in Ukraine," 4.

63 For example, see the following about the problem of the quantity of information sources which arises from different geographical operational environments. Lomas, "Weaponizing Truth," 5.

64 See the following about examples of this point. Alexa O'Brien, "Open-source intelligence May Be Changing Old-School War," *Wired*, May 24, 2022, https://www.wired.com/story/open-source-intelligence-war-russia-ukraine/?utm_source=twitter&utm_medium=social&utm_campaign=onsite-share&utm_brand=wired&utm_social-type=earned; Benjamin Strick, "Follow the Russia-Ukraine Monitor Map," Bellingcat, February 27, 2022,

https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/; Digital Security Unit of Microsoft Corporation., "Special Report: Ukraine：An Overview of Russia's Cyberattack Activity in Ukraine" (Microsoft Corporation., April 27, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[65] See the following references for the disputes regarding the value of the remaining classified information sharing by intelligence agencies even after the value of OSINT has grown, in particular the example of "intelligence diplomacy" among NATO members and the functions of the secrecy of initiatives by government institutions in a context which goes beyond the military invasion this time. Joshua Rovner, "Intelligence and War: Does Secrecy Still Matter?" *War on the Rocks*, May 23, 2022, https://warontherocks.com/2022/05/intelligence-and-war-does-secrecy-still-matter/; Allison Carnegie, "Secrecy in International Relations and Foreign Policy." *Annual Review of Political Science* 24, no.1 (May 2021): 213-33.

[66] This phenomenon has been continuous and most salient in some fields, such as the field of counterterrorism cybersecurity. See the following. Ciaran Martin, "The Development of the United Kingdom's Cyber Posture," in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest,* ed. Robert Chesney and Max Smeets (Washington, DC, Georgetown University Press 2023) pp. 201-221.; Dylan and Maguire, "Secret Intelligence and Public Diplomacy," pp. 34-35, pp.41-42. ;Petersen, "Three Concepts of Intelligence Communication," 322–25.

67 See the following as references for the trajectory of the US and the UK intelligence apparatus in recent years. Jeremy Fleming, "Director GCHQ's Speech on Global Security amid War in Ukraine" (Australian National University, March 31, 2022), https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine; Mathew J. Schwartz and Ron Ross, "Intelligence Agencies Seek Fast Cyber Threat Dissemination," *Bank Info Security*, April 25, 2019, https://www.bankinfosecurity.com/intelligence-agencies-seek-fast-cyber-threat-dissemination-a-12415.

68 See the following about the growing public-facing nature of the national intelligence services vis-à-vis emerging security challenges in the contemporary information environment. Dennis Broeders, Sergei Boeke, and Ilina Georgieva, *Foreign Intelligence in the Digital Age. Navigating a State of "Unpeace,"* The Hague Program For Cyber Norms Policy Brief (Hague: The Hague Program for Cyber Norms/Leiden University, 2019); Jamie Collier, "Getting Intelligence Agencies to Adapt to Life Out of the Shadows," *NetPolitics* (blog) (Council on Foreign Relations, April 5, 2017), https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows; Harrington, "Intelligence Disclosures in Ukraine."

69 See the following regarding this point. James Lockhart and Christopher R. Moran, "Principal Consumer: President Biden's Approach to Intelligence," *International Affairs* 98, no. 2 (March 7, 2022): 552–54; Rory Cormac, *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy*, 1st ed. (Madison Avenue; New York: Oxford University Press, 2018), 7–15; John Hardy, "Hunters and Gatherers: The Evolution of Strike and Intelligence Functions in Special Operations Forces," *International Journal of Intelligence and CounterIntelligence* 36, no. 4 (October 2, 2023): 1143–63; Stout and Warner, "Intelligence Is as Intelligence Does."

防衛研究所 National Institute for Defense Studies
NIDS Commentary
No. 224 May 26, 2022
(Updated: October 31, 2023*)

PROFILE

SETO Takashi (Mr. /he/him)

Research Fellow, Cyber Security Division, Policy Studies Department

Field of expertise: Intelligence Studies, Cyber and Information Warfare, European Security.

Planning and Coordination Office

National Institute for Defense Studies
Telephone (direct) : 03-3260-3011
Telephone (general) : 03-3268-3111 (ext. 29177)
National Institute for Defense Studies website: www.nids.mod.go.jp