

***Georgia and NATO:
A Democratic Framework for Responding to the Totalitarian Information Space***

Alexander MacDonald, National Dong Hwa University, Taiwan

The European Conference on Arts & Humanities 2023
Official Conference Proceedings

Abstract

Marked efforts to spread disinformation within Europe and NATO-allied nations has risen, not uncoincidentally, alongside a rise in totalitarian narratives and neo-imperial ambitions from the Russian Federation. Although Georgian political leaders and NATO have both worked independently to pushback against totalitarian narratives in the information space, the Substantial NATO-Georgia Package (*SNGP*) has not explicitly aimed to intertwine Georgian leadership, voices, and experience in resisting totalitarian narratives. The limited inclusion of Georgia in NATO-allied information space exercises or frameworks is a missed opportunity to create a larger joint-framework that resists anti-democratic narratives across NATO allies, and the larger democratic world as anti-democratic forces often align in spreading totalitarian messaging aimed at undermining democratic-institutional integrity. This paper presents a conceptual understanding of the totalitarian information space as totalitarian-institutions' advances to undermine the *vita activa* of the democratic information space, analysing specifically the way totalitarian narratives undermine the free exchange of information; or, the *sensus communis*. Building off this conceptual understanding, this paper then analyses the *SNGP* regarding Georgia's information space capacities and proposes a theoretical and practical model for including Georgia in combatting totalitarian information space advances. The theoretical model pursues identifying the typology of threats from a threat-analysis model, focusing on totalitarian narratives utilised. The practical model then assesses the *SNGP* and related training implemented since the document's release against NATO's 2022 capability framework for fighting disinformation to identify weaknesses and propose a triad-defence model which covers current gaps in the *SNGP*.

Keywords: Totalitarianism, NATO, Information Space, Georgia, Threat-Analysis

iafor

The International Academic Forum
www.iafor.org

Introduction

Information warfare and the proliferation of fake information have become a prominent, if not the prominent theme, of anxiety regarding democracy. If anxiety towards democracy in the Cold War chiefly concerned fascism and the spread of totalitarian regimes, the information domain now rests as the mantel piece of democratic anxiety. Writing on totalitarianism and empire, Hannah Arendt's warnings in *Origins of Totalitarianism* (1951) and Carl Friedrich and Zbigniew Brzezinski's *Totalitarian Dictatorship and Autocracy* (1956) have found a sudden, new place in a world where totalitarian regimes have digital tools to proliferate machines of unreality. These new tools allow totalitarian regimes to control information spaces through bureaucratic information warfare.

In Europe, the priming of that unreality machine has come from a host of actors globally (Singer & Brooking, 2018). However, one source – the Russian Federation – has amplified fake and weaponised information over the past decade with kinetic effect in Eastern Europe (Blankenship et al., 2022; Freelon & Lokot, 2020). The 2022 invasion of Ukraine came on the back of an elongated information war that, although some historians may date to the fall of the Soviet Union, specifically originated following the 2014 invasion of Crimea (Darczewska, 2014; Jaitner, 2015; Kofman et al., 2021; Wilde & Sherman, 2022).

As any modern war, the defence of Ukraine since 2014 has come within three specific domains: kinetic, cyber, and information (Kofman et al., 2021). Although Ukraine is not a NATO member, NATO's support within all three realms has aided the national defence. With focus on the information space, NATO's aid to Ukraine has highlighted the importance of the alliance defending its members and allied democracies from information warfare (Vitalii et al., 2022). Although NATO has long conducted studies on information warfare, ardently so following the invasion of Crimea (Thornton, 2015), they ought to turn to smaller allied-states from the former Soviet Union to inquire upon a rich history of experience facing imperial Russian information warfare.

Former soviet-bloc nations have a myriad of experience contesting, at local levels, imperial Russian disinformation in the soviet era (Applebaum, 2012). Although the current wave of Russian disinformation utilises digital tools, NATO should not dismiss or ignore the experiences of these nations. Specifically, this paper focuses on Georgia, a partner nation of NATO that has agreed to join the alliance. Georgia is a nation that, like Ukraine, has shown support for enhancing democracy and uprooting corruption. Also, like Ukraine, Russia invaded Georgia in 2008 and retains occupation of zones, despite the international community not recognising Russia's claims.

However, the *Substantial NATO-Georgia Package (SNGP)* vaguely assigns resources to combatting information warfare; nor does it have structural or institutional frameworks for assisting Georgia, or bringing Georgia into a network to combat weaponised information. Georgia's limited inclusion opens a threat to Georgia while NATO misses on the nation's experience in combatting weaponised information at the local level. Hence, there is a need for an explicitly democratic-oriented defence framework for the *SNGP* that integrates Georgia's experiences and NATO's expertise in information warfare defence.

This paper draws upon the *vita activa* as an ontological view of human activity. This ontological view informs a framework in which totalitarian states utilise narratives to mobilise society to circumnavigate a rise of the *communis sensus*. Thereafter, a threat

analysis is completed to identify typologies of information warfare threats to the Georgian polis. Moreover, a comparison between the *SNGP* and NATO's 2022 capability framework for fighting disinformation identifies missing components in the *SNGP*. To mitigate the identified threats to Georgia and the weaknesses of the *SNGP*, this paper concludes by proposing a defence-triad framework for information warfare that applies specifically to NATO and Georgia, while offering insight for democracies under threat.

Literature Review

Georgia in Information Warfare

On 7 August 2008, Georgian forces responded to violence from South Ossetian separatist units by taking control of separatist headquarters. On 8 August, the Russian military, under the premise of a "peace enforcement operation", illegally invaded Georgia via air, land, and a naval blockade. While falsely accusing Georgians of committing genocide, Russian-backed militias destroyed ethnic Georgian villages, driving Georgians from the regions of South Ossetia and Abkhazia. On 12 August, French president Nicolas Sarkozy, on behalf of the European Union, negotiated a ceasefire with Russia.

In the immediate aftermath of the conflict, a European Union Committee found Russia continued to break the terms of the ceasefire (European Union Committee (EUC), 2009 p. 9). To this day, Russia continues to illegally occupy South Ossetia and Abkhazia. Moreover, even in testimony critical of Georgian President Mikheil Saakashvili leading up to the conflict, intelligence indicated that Russia had mobilised troops on the Georgian border and prepared the information space for conflict preceding Georgian troops taking the South Ossetian separatist headquarter (EUC, 2009, p. 6). The information war began before the kinetic conflict with Russian agents distributing Russian passports to Georgians in South Ossetia and Abkhazia, attempting to create a *Casus Belli* (EUC, 2009, P. 12).

During the conflict stage, Russian cyber forces initiated cyber-attacks which defaced websites and prevented Georgian citizens from accessing critical information (Blank, 2017). Moreover, this suggested preparation stage for an invasion of Georgia, opposed to the Russian narrative of a rapid 'humanitarian' response. Moreover, Russia and Georgia each attempted to control the narrative stream by making their respective representatives available to the media. Russia used military officers on live television to present a controlled narrative of the 'humanitarian' side of Russia's cause. Although this was a rather rudimentary campaign compared to future operations, it was particularly effective in furthering Russian information warfare strategy, as well as showcasing the urgent need to defend against Russian information attacks (Blank, 2017).

The information warfare in Georgia, however, has historical connections to contested cultural memory rising from Russian Imperial ambitions (Poellath, 2021; von Beyme, 2014). Issuing Russian passports is not a mere modern trick to provide a *cassus belli* under international law; rather, connects to more historic claims over Georgian territory and Georgian culture. The Russian passport carried a cultural implication. The information warfare in Georgia draws on cultural memories of an era in which the Soviet Empire ruled Georgia. The modern information warfare attempts to transform the society from that of a 'democratising' Georgia to a 'Russian-influenced' state (Deutsch, 1966). This ultimately forms in what Russian President Vladimir Putin has called a difference in *духовные ценности* (spiritual values) between the 'democratic west' and Russia (Jaitner, 2015). That is, Russian information

sources claim a democratising Georgia is degenerate and breaking from Russian spiritual values, and thus there must be a return to Russia's sphere of influence to 'heal' society. This unique Georgian context is thus why NATO must make Georgian leadership a critical component of information warfare defence.

Substantial NATO-Georgia Package (SNGP)

NATO and Georgia formalised the *SNGP* at the 2014 Wales Summit, recognising Georgia's improvements in democracy and anti-corruption on its path to joining NATO, and Georgia's long-standing cooperation with NATO. Throughout the early years of regaining independence, Georgia joined multiple partnerships, participated in the NATO-Georgia Commission, and became an Enhanced Opportunity Partner (eOP). Italy has become a key member of this partnership, both with its Navy and through training of the Georgian Military Police (Iorio, 2021). Moreover, the 1994 *Science for Peace and Security Programme* expands cooperation to non-defence and military aspects, such as disaster mitigation, science and research development, and infrastructure construction (Iorio, 2021).

The 2014 *SNGP* supported 15 areas and offers a 'comprehensive' approach to strengthen strategic, tactical, and operational cooperation between NATO and Georgia. Through the package, Tbilisi opened a *NATO-Georgia Joint Training and Evaluation Centre* and the *Georgian Defence Institution Building School*. In 2020, NATO approved an upgraded *SNGP*, covering 16 domains, including cyberspace. Currently NATO is assisting Georgia in training and equipping their military with NATO-standard equipment, upgrading from Soviet technology (NATO, 2023).

However, the packages do not outline any specific plans in defence of information warfare. Although NATO recognises that Georgia's inclusion is critical due to a present threat from Russia, and NATO scholars repeatedly draw on 2008 for lessons about information warfare (i.e., Jaitner, 2015), there is no explicit outline for improving information warfare defence. Georgia has participated in information defence exercises in the past five years. However, without a plan for explicit formulation of defending the information space, both Georgia and NATO lose critical value to defending civilians and Georgia's democratic progress.

A Concept of Totalitarian Narratives

The following section outlines an existential ontological reflection of Hannah Arendt's *Vita Activa* to begin a sketch of totalitarian narratives from an ontological perspective. Although Arendt's *Vita Activa* does not connect directly to totalitarianism, the intent of outlining this ontological view is to provide the existential lens through which this paper views totalitarianism. Then, a functional view of the totalitarian information space as a series of narrative tools to attack and restrict a free information space.

- Vita Activa and Sensus Communis

Hannah Arendt's *The Human Condition* (1958) is a summary and defence of the *Vita Activa*, or, the Active Life – a contrast to the *Vita Contemplativa* (The Contemplative Life) and the *stasis* of thinking. The *Vita Activa* proceeds through labour (the biological processes of life), work (human creativity in the natural world, creating lasting objects in the public sphere), and action (human engagement and communication, which generates political action). In action, the political life of action generates praxis, which allows for a plurality of ideas. This

plurality is essential to the ontological view of the political life, the lens for observing the formation of human activity. As Arendt writes in her more neglected book *On Revolution* (first published 1963):

The grammar of action: that action is the only human faculty that demands a plurality of men; and that syntax of power: that power is the only human attribute which applies solely to the worldly in-between space by which men are mutually related, combine in the act of foundation by virtue of the making and the keeping of promises, which, in the realm of politics, may well be the highest human faculty. (1990, p. 175)

That is, action requires a plurality, and by connection, a trust of promises kept between humans. Action in the *Vita Activa* form the freedom to start something new. In the political realm, thus, a consensus to start something new requires promises (Arendt, 1958). The ability to promise, thus, requires a space in which humans can entrust one another and confirm a consensus of promises.

This is, briefly, where a line connects between the *vita activa* and democracy, and thus, totalitarianism. Ontologically, a space for the ‘miracle’ of the new to occur is essential to a ‘democratic’ system, if ‘democracy’ is the plurality of humans acting in-between the private and public space to form and maintain promises. This also draws closely, and highlights the importance of, the *sensus communis*. Hence, the *Sensus communis* as community sense becomes the core of the political life; communication, forming promises, in the *polis* forms the political life (Degryse, 2011; Norris, 1996). However, opposed to an ‘empirical’ reading of Arendt (i.e., Beiner, 1997; Norris, 1996), this paper maintains the concept of the *sensus communis* (Degryse, 2011) as not only ‘community sense’, but ‘[political] sense formed by communication.’ Or, action (communication and information) forms the *sensus communis*.

The formation of *sensus communis* as ‘[political] sense formed by communication’ allows for an ontological view which places a role of communication in the political life of action. Thus, this communication properly placed in the political life allows for a line to information and thus allows for a formalisation of the role in which information forms a democratic society. By contrast and the inverse principles, totalitarian bureaucracies must thus operate to interrupt the *sensus communis* and mobilise the *polis* towards the regime’s machinery.

- ***The Bureaucracy’s Mobilisation of the Polis***

The conceptualisation of the *vita activa* and *sensus communis* only makes attempts to define an existential political view, without making substantial claims on democracy or totalitarianism. It informs something about such systems, and this section will expand upon those formations. These, however, are an extension of Arendt’s work, utilising the expanded version of her political lens above to observe and thus say something more about totalitarianism and information.

For both Karl W. Deutsch (1954, 1966) and Arendt (1951) bureaucracy was a form of empire and totalitarianism that served specific purposes for destroying the political life. The role of bureaucracy served empire and totalitarian states to enforce control or terror. Bureaucracy is the entrenched organisations that enforce either an isolated political life (destroy the in-between of the private and public sphere) or serves to command terror on communities (Arendt, 1951; Villa, 1999). The bureaucracy controls the definitions of culture and society

through controlling the information, and thus retaining control of communication and information.

The *sensus communis* is essential to action, as this is where new ideas through the political life become verified through judgement. Hence, the claim made that the *sensus communis* is the '[political] sense formed by communication'. Extending through this a *polis* with liberty, that is the spaces for praxis, has *sensus communis*. Hence, the role of the totalitarian bureaucracy is to close spaces and define the operations of the *polis*. The political action (and thus active life), in totalitarianism, shifts to the totalitarian bureaucracy.

However, as Deutsch (1954) defines, totalitarianism occurs in an ideology-strong regime; authoritarianism occurs in an ideology-weak regime. This is a critical distinction, as in authoritarianism, the regime pushes the *polis* (if it can even retain such a title) towards merely closing spaces; the bureaucracies act as agents mobilising away from political challenges towards the regime. Totalitarian bureaucracies mobilise towards an ideology, and thus assume the formation of the community sense by altering communication. Totalitarianism interrupts the communicative process via noise, and thus utilises totalitarian narrative tools to interrupt the process of forming consensus and verifying political judgement.

Hence, there is a reason in the introduction did not utilise the terms *disinformation* or *propaganda* and maintained only *information warfare* or *weaponised information*. Disinformation or propaganda are merely one of many possible tools. The totalitarian regime must destroy the ability to make promises, or form free consensus, and mobilise that power towards enacting the regime's will. Having briefly reviewed the context of Georgia and information warfare, in addition to the *SNGP*, and conceptualising totalitarian narratives through the *sensus communis*, the following section outlines the threat-analysis formation to identify the specific forms of totalitarian narrative tools which threaten Georgia specifically, and later how aligning the *SNGP* to the *NATO Capability Framework* will shudder the tools of Russia's totalitarian bureaucracy.

Method

This section outlines the method and strategy to studying the threats posed to Georgian's *polis* via information warfare and a brief note on comparing the *SNGP* and *NATO Capability Framework*.

Threat-Analysis: Narrative Typologies

Bruce Schneier first developed the interdisciplinary Attack Tree framework in 1999 primarily for the cybersecurity realm (Schneier, 1999). By modelling threat vectors and attack avenues, defenders can identify risks and develop associated mitigation vectors and costs. Operators "or" and "and" denote that to complete the higher attack in the tree, attackers must achieve one or both objectives. The attack tree continues to see utilisation in the security domain and as the core for development of newer identification models (e.g., Deng et al., 2011).

Schneier's Attack Tree allows for the development of a framework of direct threats to the Georgian *polis*. Consequentially, the threat analysis reveals mitigation paths which the proposed defence triad can thus mitigate.

NATO Information Warfare Capability Framework

The NATO 2022 Capability Framework (Pamment, 2022) outlines a definition of capabilities, assessments, and countermeasures to counter disinformation and information influence. The framework divides counter-disinformation capabilities into countering capabilities (8 categories) and public resilience (4); counter-information influence capabilities into ‘analysis and identification’ (7) and strategic communication (5); counter-foreign interference (5); intelligence and security policy (7); system-wide capabilities into country systems (6); ‘partnerships and alliances’ (3); and professional development (3). There are 48 categories included in the framework.

Table 1 displays these capabilities with a “yes” for capabilities the compendium of the *SNGP* and Georgian-NATO have fulfilled, no for those which not completed, and a partial for those half-implemented. Partially are assumed to have a framework on the way to completion, and thus are counted as ‘completed’ below. The *SNGP* is, as the differences between the 2014 and 2020 version highlight, an evolving package as new threats, and training opportunities, emerge.

| | | | | | |
|--------------------------------|------------------------|-----------------------------|------------------------|--------------------------------|------------------------|
| Countering Capabilities | <i>SNGP Inclusion?</i> | Public Resilience | <i>SNGP Inclusion?</i> | Analysis Identification | <i>SNGP Inclusion?</i> |
| Content Moderation | No | Public Awareness | Yes | Monitoring | Yes |
| Content Flagging | Yes | Media Literacy | Partial | Situational Awareness | Yes |
| Content Labelling | Yes | Source Criticism | No | Threat Assessment | Sector3* |
| Content Demotion | No | Pre-debunking | No | Risk Assessment | Sector3* |
| Debunking | Yes | | | Investigation | Sector3* |
| Fact-checking | Yes | | | Tabletop Exercises | Yes |
| Counter Messaging | No | | | Partnerships | Yes |
| Elves (anti-troll ops) | No | | | | |
| Strategic Communication | <i>SNGP Inclusion?</i> | Intelligence | <i>SNGP Inclusion?</i> | Security Policy | <i>SNGP Inclusion?</i> |
| Proactive Communication | No | Analysis and identification | Yes | Deterrence | No |
| Counter-narratives | Yes (e.g., Covid-19) | Oversight | Yes | Exposure | No |
| Counter-brand | Sector3* | Intelligence Sharing | Yes | Attribution | Yes |
| Published-analysis | Sector3* | OSINT | No | Network disruption | No |
| Attribution | No | Counter intelligence | No | Legislation | No |
| | | | | Sanctions | Yes |
| | | | | Offensive Operations | No |

| Country Systems | <i>SNGP Inclusion?</i> | Alliances | <i>SNGP Inclusion ?</i> | Professional Development | <i>SNGP Inclusion ?</i> |
|----------------------------------|------------------------|-------------------|-------------------------|---------------------------------|-------------------------|
| Research & Development | Science initiatives | NGO Partners | Sector3* | Guidelines | Unknown |
| Legislation, regulation & policy | No | Joint initiatives | Yes | Specialism | Unknown |
| Measurements & evaluation | No | Common Goods | Yes | Exchanges | Unknown |
| Coordination | No | | | | |
| Civil | Sector3* | | | | |
| Defence | | | | | |
| Vulnerability analysis | Yes | | | | |

*Sector3 is a key democracy and information Georgian NGO which cooperates with the European Union and NATO

Table 1: Summary of NATO Capability Framework

The *SNGP* and extended NATO partnerships with Georgia fulfil 4 of 8 countering capabilities; 2 of 4 public resilience capabilities; 7 of 7 ‘analysis and identification’ capabilities; 3 of 5 strategic communication capabilities; 3 of 5 intelligence capabilities; 2 of 7 security policy capabilities; 3 of 6 country system capabilities; 3 of 3 ‘partnerships and alliances’ capabilities; professional development guidelines are unknown. In total, the *SNGP* and partnerships fulfil 27 of 45 capability categories while 3 remain unknown.

Results

Threat-Analysis and Missing Gaps in SNGP

The threat analysis framework utilised the literature review in the second section (e.g., Blank, 2017; EUC, 2009, Jaitner, 2015; Poellath, 2021) alongside threat developments under the Russian invasion of Ukraine to develop a threat-analysis framework (Atlantic Council, 2023; Blankenship et al., 2022; Serpanos & Komninos, 2022; Wilde & Sherman, 2022). Figure 1 displays the threat tree framework to the Georgian *polis*.

The threat analysis formulates around top level threats legislative subversion, media information influence, and cultural narratives. These three top level threats display more existential threats with the direct threats in the attack chains below. Notably, corruption, election interference, and anti-democratic legislation form the legislative subversion aspect. Georgia has felt the threats of corruption and general interference previously, and in a democratising nation, form a particularly potent threat (Taliuri et al., 2020) Introducing corrupt politicians willing to introduce anti-democrat legislation or divide the *polis* through media influence represent a continued existential and functional threat to Georgia.

Second, media information influence is a direct threat to dividing and sparking violence and distrust in the plurality of Georgia. With high levels of violence and division among the society, normal democratic institutions cannot assist in providing a space for *sensus*

communis. The influence does not need to contain complete coherency, but can (as noted in the *or* node) be anti-Georgian narratives or pro-Russian cultural narratives.

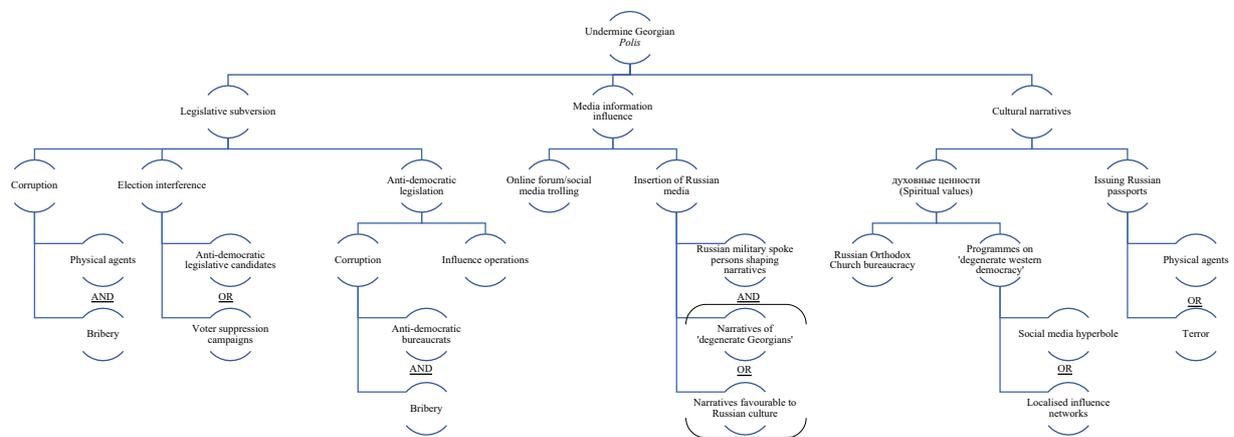


Figure 1: Threat Analysis Framework to Georgian Polis

Lastly, cultural narratives pose the most significant threat. This includes narratives around the *spiritual values* of Russia, including threats from the Russian Orthodox Church sending agents of division disguised as holy men. As seen in Ukraine throughout the invasion, priests and leaders in the Russian Orthodox Church have accompanied occupiers, presenting narratives of ‘western’ degeneracy and, at times, acting as spies. Cultural narratives in a society with deep scars from past violence and divisions can open old wounds not entirely forgotten or healed. The confusion of the memory and trauma under the USSR can easily open new wounds at times of elections or democratic reforms.

Collectively, however, there are common themes across these categories: corruption, media influence, and cultural division. Corruption and cultural division present the most significant threats. Both threats present localised challenges, which only Georgian experts can identify and mitigate. Moreover, corruption is a challenge which legislation has targeted effectively, yet presents an ever-looming threat; even the oldest democracies must protect themselves against corruption and bribery.

- **Missing gaps in the SNGP**

The *SNGP* with other documentation and training present a solid beginning to NATO and Georgia’s relationship at addressing and defending from information warfare. However, with only 26 of the 45 capabilities fulfilled, Georgia and NATO’s defence has work left to complete. Notably, *Sector3* plays a significant role in enhancing the collaboration between Georgia and NATO. Yet, as the 2023 factsheet states, “More of Georgia in NATO, and more of Georgia in NATO,” there seems little of ‘Georgian expertise in NATO’. Threat-intelligence, exercises, and documentation (i.e., reporting on Covid-19 disinformation) all play significant roles.

The current framework lacks Georgia’s expertise in NATO, pre-debunking, common media literacy beyond a theoretical basis (Basilaia & Danelia, 2022), legislation, and network disruption. Hence, there is a lack of offensive posturing in the relationship between NATO and Georgia in addressing information warfare. Moreover, efforts are *not* localised in the *SNGP* and instead have become spread across different alliances and departments. There remains a lack of a forward operating posture which addresses forming threats and pre-debunking influence operations. Moreover, NATO should operate and supply larger funding for localised combat against information influence. Outlying villages and rural areas possess a unique risk as while urbanite social media may not influence these communities, text-chains, cyber fraud, threats, misrepresentations of the war in Ukraine, and rumours of violence could harm these communities.

Hence, there remains a need to centralise efforts into a democratic defence-triad which focuses again on the existential reality of a *sensus communis* and a *polis*. Information warfare, unlike kinetic warfare (which often, although not always), targets civilians and the *polis* first and foremost. By destroying the spaces, or the trust in spaces where the *sensus communis* occurs, then democracy and an open society dissolve. In its place, totalitarianism and an ideology of fear and subservience may rise.

Re-aligning Threats and Gaps: A Democratic Defence-Triad for Georgia

This paper, unfortunately, cannot address the specific organisations and legislation which Georgia ought to pass. However, by proposing a democratic defence-triad, based on mitigating the threats above, scholars, activists, and policy-makers might begin to address issues from a perspective that focuses on the *formation of political sense* which information warfare most directly affects. Figure 2 displays the Information Warfare Defence-Triad.

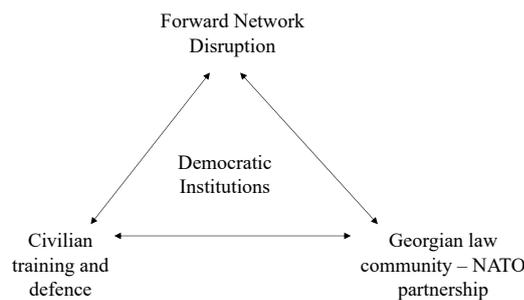


Figure 2: A democratically based information warfare defence-triad

The core of the triad is the democratic institutions as the core of the society and institution which the triad defends. Democratic institutions are core to the integrity and success of the model; without these institutions the model itself becomes merely bureaucracy. The design involves stakeholders of the democratic process and the institutions themselves: civilians, the lawyers who uphold the law, and an offensive component in which multiple bodies may

participate. Critically, all these components work in unison and coordinate, mitigating the rather disconnected and uncoordinated measures which NATO and Georgia have currently taken.

The civilian training and defence component fulfils components of media literacy, NGOs, identifying, public awareness, and pre-debunking. The civilian component thus directly involves the most critical stakeholders of the defence triad. Moreover, the civilian component ought to directly involve community members outside of the urban capitals of democracy; those rural communities who long-memory of cultural conflict, terror, disinformation and confusion might more directly affect. The *SNGP* and partnership between Georgia and NATO ought to involve in mitigating this lacking leg of the triad first.

Second, forward network disruption is critical to a proper defence. This allows for insight into the objectives and structures of opponents, giving the defenders crucial information to establishing a forward and pre-bunking posture. Disinformation is similar to a contagion, and once in the community, is difficult to stop. Thus, forward hunting and network disruption is a critical leg to allowing civilian defenders to communicate information to the community and for the legal team to review and establish proper recommendations to the legislative bodies. Moreover, forward hunting cooperation in the “more of Georgia in NATO” kind will provide the rest of Europe critical expertise and context for how some Russian cultural, weaponised information may operate.

Lastly, although this triad is in no specific order, the legal community partnership is critical to protecting against corruption, recommending appropriate (but not undemocratic laws which deprive citizens of civil rights) laws to fight disinformation and corruption, and giving legal and constitutional experts a key stakeholder position in Georgia’s most important international alliance. This body will also enhance NATO leadership’s understanding of Georgian law and the democratisation process, giving critical context to the defence of democratic processes and institutions.

Hence, this proposed triad retains the concepts, processes, and institutions of democracy at its core, while incorporating a legal expert body, a forward operating and threat hunting body, and a civilian defence body which the information warfare-defence partnership between NATO and Georgia can be reshaped around.

Discussion and Conclusion

Implementing an Information Defence-Triad for Georgia and NATO

Implementing a defence-triad is critical to organising and fulfilling the structural intentions and needs of the Georgia and NATO partnership. The information defence-triad incorporates key stakeholders and democratic bodies, while mitigating the current gaps in the *SNGP* and threats to Georgia. This, however, does not indicate any such implementation does not raise key challenges moving forward.

The foremost challenge, and threat which no academic framework can solve, is strong, democratic leadership at the community level. The second leg of the triad relies on civilian defence, pre-debunking, and media literacy. However, without strong leadership among educators, researchers, and community stakeholders, this leg will not uphold the remainder of the triad. Retaining community attention and interest remains a critical challenge moving

forward. Researchers and experts should move forward in investigating effective methods of teaching media literacy and expanding the buy-in from the *polis*.

The second challenge is the effect of a legal oversight committee should more authoritarian politicians find their ways into power. This remains not a threat only in Georgia, but any democratic nation; regardless of the age of that democracy. Pro-active anti-corruption legislation and practice, which Georgian lawmakers have implemented, remains key to mitigating immediate threats to the democratic institutions. However, thousands of kilometres away, Hong Kong remains a persistent warning for Georgia. There existed a strong pro-democracy legal oversight body, with hundreds of lawyers who fought to defend paths to democratising Hong Kong. However, a totalitarian government swept them aside, changing the rules to favour the regime and make a mockery of the rule of law (Tai et al., 2020). Georgia and Hong Kong are in very different places in their history; however, the triad cannot lose the importance of lawyers who have an influence in the information war and its relevant laws.

Implications and Functions for Non-NATO Nations

The gaps in defence and threats to Georgia, based on an ontological framework of the *sensus communis* as the core of the political life, crafted the proposed framework. However, the framework is relevant and adaptable to any democratising, or democratic nation. The broad institutions, and the sacred formation of the *sensus communis*, form the core of the framework. Whether a NATO nation, who each body will involve an international alliance and partnership, or a non-NATO nation such as Taiwan, this proposed framework addresses deep and lingering concerns.

No framework, however, cannot address all the functional concerns of the invasion of a totalitarian information space. Yet, by maintaining the core spirit of the *sensus communis*, any democracy has a chance to maintain a strong triad of institutions which can allow for a free development of its *polis*.

Conclusion

This paper has approached several subjects key to democracy and the defence of democracy (defence against information warfare), aiming to open a key contribution to an area of immediate concern to Georgia and nations beyond. By conceptualising the *sensus communis* as ‘[political] sense formed by communication’, the contrasting totalitarian information space, which aims to close these communication channels (or judgement and consensus formation channels) through noise. This noise is weaponised information.

The NATO-Georgia *SNGP* offers a remarkable chance to defend against information. Thus, an analysis thereafter identifies gaps in the *SNGP* – summarised as legislative, forward operation capabilities, corruption, and civilian defence. A threat analysis constructs a mature understanding of the most immediate threats to Georgia’s *polis* – summarised as corruption, weaponised media influence, and cultural divisions. With relevance to these concerns, this paper proposes a novel information warfare defence triad with democratic institutions at its core, and a civilian training defence body, a lawyer oversight body, and a forward operating team forming its legs. While this model addresses formalising these three bodies within the Georgia-NATO partnership, any democratic nation can utilise this defence triad for a

formalising of its domestic or international defence posture and institutions towards information warfare.

Acknowledgments

Thank you to the comments and experts at ECAH 2023 for providing comments which aided the final version of this paper. Thank you to the help from advisor and Professor Markus Porsche Ludwig. This paper is dedicated to, and inspired by, the bravery of the Ukrainians and Georgians fighting against totalitarianism. To all those fighting totalitarianism: *Heroaim Slava*.

References

- Applebaum, A. (2012). *Iron curtain: the crushing of Eastern Europe 1944-56*. Penguin UK.
- Arendt, H. (1951). *The origins of totalitarianism*. Houghton Mifflin Harcourt.
- Arendt, H. (1958). *The Human Condition*. Chicago: University of Chicago Press.
- Arendt, H. (1990). *On Revolution*. London: Penguin Books.
- Atlantic Council. (2023). *Our experts decode the Putin speech that launched Russia's invasion of Ukraine*. Atlantic Council. Retrieved 23 February 2023 from <https://www.atlanticcouncil.org/blogs/new-atlanticist/markup/putin-speech-ukraine-war/>
- Basilaia, E., & Danelia, N. (2022). *Mapping and needs assessment of media literacy practices in Georgia*. Council of Europe. <https://rm.coe.int/-en/1680a5789e>
- Beiner, R. (1997). Rereading Hannah Arendt's Kant Lectures. *Philosophy & Social Criticism*, 23(1), 21-32. <https://doi.org/10.1177/019145379702300102>
- Blank, S. (2017). Cyber war and information war a la russe. *Understanding cyber conflict: Fourteen analogies*, 1-18.
- Blankenship, M., Saladino, C. J., & Brown Jr, W. E. (2022). Ukraine-Russia War: Nevada Twitter and Disinformation Trends.
- Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study*. OSW Ośrodek Studiów Wschodnich im. Marka Karpia.
- Degrise, A. (2011). Sensus communis as a foundation for men as political beings: Arendt's reading of Kant's Critique of Judgment. *Philosophy & Social Criticism*, 37(3), 345-358. <https://doi.org/10.1177/0191453710389452>
- Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011, 2011/03/01). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1), 3-32. <https://doi.org/10.1007/s00766-010-0115-7>
- Deutsch, K. W. (1954). Cracks in the Monolith: Possibilities and Patterns of Disintegration in Totalitarian Systems. In J. F. Carl (Ed.), *Totalitarianism* (pp. 308-342). Harvard University Press. <https://doi.org/doi:10.4159/harvard.9780674332621.c24>
- Deutsch, K. W. (1966). *Nationalism and social communication: an inquiry into the foundations of nationality*. Cambridge: MIT Press.
- (EUC) European Union Committee (2009). *After Georgia, The EU, and Russia: Follow-Up Report: Report with Evidence*. House of Lords.

- Freelon, D., & Lokot, T. (2020). Russian Twitter disinformation campaigns reach across the American political spectrum. *Misinformation Review*.
- Friedrich, C. J., & Brzezinski, Z. (1956). *Totalitarian Government and Autocracy*. Cambridge, Mass.: Harvard University Press.
- Iorio, N. (2021). Lens on NATO-Georgia Cooperation: A Shared Engagement. In F. L. Bonali, F. Pasquaré Mariotto, & N. Tsereteli, *Building Knowledge for Geohazard Assessment and Management in the Caucasus and other Orogenic Regions* Dordrecht.
- Jaitner, M. (2015). Russian information warfare: Lessons from Ukraine. In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 87-94). https://www.ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf
- Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J., & Waller, J. (2021). *Russian Military Strategy: Core Tenets and Operational Concepts*. https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf
- Kotsur, V., Maletych, M., Pogrebytskyi, M., Negoda, A., Trachuk, T., & Andriushchenko, M. (2022). Ensuring National Security in Conditions of War: NATO's Influence. *Economic Affairs*, 67(4), 707-714. <https://doi.org/https://doi.org/10.46852/0424-2513.4s.2022.4>
- NATO. (2022). *The Substantial NATO-Georgia Package, Factsheet, February 2022* https://web.archive.org/web/20230404223703/https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/Strategic-Communications-georgia.pdf
- NATO. (2023). *Relations with Georgia*. Retrieved 12 April 2023 from https://web.archive.org/web/20230527100508/https://www.nato.int/cps/en/natohq/topics_38988.htm
- Norris, A. (1996). Arendt, Kant, and the Politics of Common Sense. *Polity*, 29(2), 165-191. <https://doi.org/10.2307/3235299>
- Pamment, J. (2022). *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference* (978-9934-619-13-7). NATO Strategic Communication Centre of Excellence.
- Poellath, M. (2021). Agents, fascists and provocateurs: disinformation as an instrument to delegitimize uprisings in Eastern Europe (1953, 1956, 1968) and its impact on the politics of memory. *Journal of Intelligence History*, 1-23. <https://doi.org/10.1080/16161262.2021.1918940>
- Schneier, B. (1999). Attack trees. *Dr. Dobb's journal*, 24(12), 21-29. <https://cse.sc.edu/~zeng1/csce790-f21/papers/attacktrees.pdf>
- Sector3. (2023). *Sector3 Hub for Development*. Retrieved May 2023 from <https://sector3.ge/>

- Serpanos, D., & Komninos, T. (2022). The Cyberwarfare in Ukraine. *Computer*, 55(7), 88-91. <https://doi.org/10.1109/MC.2022.3170644>
- Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan Books.
- Tai, B., Veitch, S., Hualing, F., & Cullen, R. (2020). Pursuing Democracy in an Authoritarian State: Protest and the Rule of Law in Hong Kong. *Social & Legal Studies*, 29(1), 107-145. <https://doi.org/10.1177/0964663919869725>
- Taliuri, L., Japharidze, M., & Lagidze, K. (2020). *Possible risks of online disinformation during election period and best international practice of risk reduction*. <https://sector3.ge/Researches/Download/505>
- Thornton, R. (2015, 2015/07/04). The Changing Nature of Modern Warfare. *The RUSI Journal*, 160(4), 40-48. <https://doi.org/10.1080/03071847.2015.1079047>
- Villa, D. R. (1999). *Politics, philosophy, terror: essays on the thought of Hannah Arendt*. Princeton: Princeton University Press.
- Von Beyme, K. (2014). *On political culture, cultural policy, art and politics*. Springer. <https://doi.org/10.1007/978-3-319-01559-0>
- Wilde, G., & Sherman, J. (2022). Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election. *Atlantic Council*, 14.

Contact email: alexanderpapers@protonmail.com