Small States & Territories, Vol. 6, No. 1, 2023, pp. 15-34

Small European states in the hybrid warfare era: The cases of Cyprus, Malta, and Estonia.

Constantinos Adamides
University of Nicosia
Cyprus
adamides.c@unic.ac.cy

and

Petros Petrikkos
University of Nicosia
Cyprus
petrikkos.p@unic.ac.cy

ABSTRACT: The increasing number and complexity of hybrid threat activities forces small states, especially those with limited access to material resources, to reassess their foreign and defence policies. While the variable of 'smallness' may be sufficient to justify their overall engagement in dealing with conventional security threats, in the hybrid arena this is not the case. Pressure is amplified in establishing or maintaining a status of a reliable mediator, partner, and strategic communicator vis-à-vis their multilateral relations with other states or organisations to which they belong. This paper focuses on how small European states, with specific reference to Cyprus, Malta, and Estonia, need to develop adjustable yet resilient policies in accommodating security needs vis-à-vis hybrid threats, that are not only pertinent to their security, but also to that of the EU bloc. As the line between war and peace becomes more blurred due to hybrid threats, the small states' security shortcomings may also become a security problem for the EU bloc. We argue that the nature of hybrid threats is such that hybrid activities can be utilised to hurt bigger states in a bloc by exploiting the small states' vulnerabilities. Both the defensive and foreign policy collaborations of small states with bigger states have been, and are constantly being, re-evaluated to tackle and prevent such problems. As such, two objectives are identified in this approach. The first is the small states' quest to appear as reliable partners within the bloc. The second is to avoid being the weakest security link in the bloc's defence against hybrid threats. This unfamiliar environment for small states prompts us to rethink security from their perspective against complex and hybrid threats, and in relation to their security role as members of large organisations such as the EU.

Keywords: conventional threats, Cyprus, defence, Estonia, foreign policy, hybridity, Malta, security, small states, unconventional threats

Introduction

Small wars and low-intensity conflict aiming at operating below the threshold of conventional warfare is not a contemporary issue or concept. Despite that, there is still an ongoing challenge in clearly conceptualising and implementing 'hybridity' in Security Studies frameworks, and even more so in policymaking circles. While remaining highly contested, the persisting issue of hybridity is widely discussed and attributed to those security issues that are mixed in nature, combining both conventional and unconventional characteristics (Treverton et al., 2018; Bajarūnas, 2020). These exceed the traditional understanding of threats deriving from an opponent's military and material superiority alone, and now include a diverse set of tactics aiming at weakening an adversary, either through information tools or by taking advantage of technological infrastructural, societal, and political vulnerability gaps. Not least due to the complexity of the issue of hybridity, academics and practitioners do not necessarily perceive or analyse the issue of hybridity the same way. Thus, the gap and lack of understanding between the two may indeed be a vulnerability itself. It is, unsurprisingly, acknowledged that there is a need to have a bridge between academia and practitioners to respond appropriately to the risks of multifaceted types of security breaches, especially in the era of 'greying' war and peace (Hughes, 2020; Bressan and Sulg, 2020).

The absence of physical, traditional, or conventional types of threats may not necessarily signify the end of a threat or the absolution of possible risks. On the contrary, it is more likely to observe risks and threats deriving from non-conventional means, which lead to questions that address blurred threats that are not easily identified on time (Suchkov, 2019, pp. 418-419). The ability to respond to non-conventional threats should be high on the agenda of all states irrespective of their size or status in the international system, and irrespective of their involvement in a conflict or not. This is also one of the security priorities and concerns of the European Union (EU) (Bajarūnas, 2020; Rehrl, 2021; Council of the European Union, 2022). Challenges from such threats are multifaceted and diverse, ranging from issues of attribution to questions of appropriate response, to methods of deterrence and resilience, to how an individual state's defence abilities and security gaps has an impact on the collective security of Blocs or other partner states.

Interestingly, while the challenge of hybrid and unconventional threats is widely discussed, there is little focus on how the same questions apply to smaller states. There is indeed a rich body of literature tackling small states and security (Keohane, 1969; Alford, 1984; Goetschel, 1998; Ingebritsen et al., 2006; Archer et al., 2014; Kennedy-Pipe and Zaidi, 2021) and extended work on conceptualising, understanding, and responding to hybrid threats, as is the case for instance, targeted disinformation campaigns on the civilian population, attacks on national critical infrastructure, social engineering, and diplomatic tactics to undermine the credibility of the state internationally. But there is limited work that focuses directly on how small states specifically formulate policies in response to such threats, or on the limitations they face in their attempt to do so.

This paper attempts to bridge this gap and offer further insights on how small states, particularly those experiencing routinely security risks, tend to structure policy in response to these risks. Specifically, we argue that they do so by breaking down and simplifying their understanding of perceived threats, splitting the problem of hybridity into questions of 'conventional' and 'unconventional' types of threats. They choose to do so for several reasons, the most important of which are: (a) it is convenient and easier for practitioners to group such threats in distinct categories; (b) it is more feasible in terms of security and resource management, given the limited material resource capabilities of small states; and (c) small states may still be developing their infrastructural capability and understanding towards managing such threats. Whether this is the most appropriate way, or simply a reckless approach towards hybridity, we argue that small states, as a coping mechanism, often opt to craft policy in this way in response to their daily security struggles. That said, there is certainly a learning curve, and there is subsequent progress in security management and in dealing more 'accurately' with hybrid threats. It should be noted that the paper does not seek to elaborate on specific hybrid threats, but rather focuses on the administrative front, as well as on the challenges in amassing both civilian and military instruments to deal with the said threats.

This case study focus is primarily on Cyprus but complements its findings with the cases of Malta and Estonia and seeks to examine how they have developed – or need to develop – adjustable yet resilient policies to accommodate security needs deriving from hybrid-threat related activities. These needs are not only pertinent to their security, but also to that of the EU bloc given that all three are member states. The latter argument is one of the central hypotheses of the paper; namely that the nature of hybrid threats is such that hybrid activities can be utilised to hurt both the small state itself, as well as bigger states in a bloc by exploiting the small states' vulnerabilities. In simple words, we examine whether in the era of 'greying threats', small states can be used as a 'Trojan horse' for bigger targets, such as the EU. At the same time, we examine how such challenges may question the credibility of a small state as a reliable security partner on a bilateral and multilateral level. Therefore, our contribution also advocates a rethink of how small states view their security role as members of a bloc such as the EU, and how the latter may view the potential vulnerabilities of the small state as a collective problem.

The paper proceeds with an overview of the conceptual framework, which includes 'smallness' as an integral variable in understanding small states' assessment of foreign and defence policies. The second major section is a discussion on small states' foreign policy vis-à-vis unconventional threats and how it overlaps with their defence policies. This section also distinguishes between small states that face an Overarching Existential Threat (OET) (e.g. Cyprus, Estonia) as opposed to those that do not (Malta), and how each perceives, and deals with, unconventional threats. Finally, we examine whether small states could potentially 'punch above their weight' in terms of becoming a valuable security partner.

The research utilises both primary and secondary literature and data on modern approaches towards understanding policy formulation for small states vis-à-vis security threats. The paper also incorporates information gathered through numerous semi-structured interviews[1] with specialists (academics) and/or practitioners directly involved in policy formulation and implementation over matters relating to security, defence and foreign policy. We corroborated and enriched the interview insights through both secondary and primary sources and government document analysis, such as official and milestone events coverage via media releases, strategy documents, legislation, governmental announcements, policy briefings, academic reports and other related literature.

Smallness and (in)security

'Smallness' is traditionally attributed to those states that are limited in a physical sense, in terms of (a) size, (b) resources, and (c) capabilities. This is something that has been excessively conceptualised in both classical and intermediate approaches (Keohane, 1969; Barston, 1973; Ingebritsen et al., 2006), as well as in more contemporary literature (Baldacchino & Wivel, 2020). While states pursue security and attempt to establish themselves in the world political arena, their role is limited by their material capabilities, including the capacity to utilise large numbers of personnel effectively, deploy defensive arsenal, as well as design and maintain an efficient bureaucratic and infrastructural build that accumulates and makes use of resources for statecraft (Thorhallsson, 2018, pp. 18-19).

While the size aspect (territorial boundaries and population) is self-explanatory, the aspect of resources can be more complex. The small states' traditional limitations (e.g., military capacity and small economies) may have an impact on the diversification of specialisations and expertise capabilities. Therefore, small states may shift their focus from their limited actual

[1] Interviews were from stakeholders in Cyprus, Estonia and Malta. See "Annex: Interviews" for a detailed description.

material power they possess (such as their military arsenal), to the actual power they exercise (such as diplomacy), which is frequently 'softer' in nature, ultimately aimed at enhancing their influence and to portray themselves more favourably in the eyes of other states (*ibid.*). This means that small states may opt for non-traditional security measures (with all the security risk that this entails), precisely because of their resource limitations and their shift of focus towards soft power goals.

Unsurprisingly, small states face more survival insecurities due to their physical limitations (Neumann & de Carvalho, 2015; Bailes et al., 2014). They may therefore find themselves in an ongoing existential trap, while simultaneously trying to showcase and project that they are reliable partners in the regional and international political arena (Rumelili, 2015). Thus, it is critical to understand how small states behave and react to security crises, and how they attempt to first construct an environment that safeguards their autonomy, and then craft and project an image of the 'self' to the international community that showcases qualities of a solid security partner with whom collaborations – and subsequently protection – may be beneficial to others as well (Lamoreaux & Galbreath, 2008; Hom & Steele, 2020, p. 328).

In their struggle to be recognised for their usefulness and potential contribution to the international political realm, small states seek a different kind of policy formulation that would allow them to have a more active role in the system. Indeed, small states are forced to rethink their security dilemmas. Specifically, it is not just about survival, but also about influence and trustworthiness, and how they can achieve this goal given their smallness (Vaicekauskaitė, 2017, p. 9, Steele, 2008, p. 14). This is even more prominent in cases where small states have joined blocs such as the EU, and where collective security is an issue that always needs to be taken into consideration along with the national security concerns.

Thus, small states that belong in specific blocs ought to prove that they can improve their capabilities and thus become more reliable and dependable partners and not free riders or, more importantly, a security risk to the bloc. For instance, the case of Cyprus shows how Chinese hackers were able to obtain access to EU policy on foreign affairs, security, enlargement, and migration, using Cypriot diplomatic credentials (Sanger and Erlanger, 2018). The breaching of credential information was not just a threat to Cyprus, but to the bloc as a whole, as revealed in the diplomatic cables that were leaked (*ibid.*). Similarly, the cyber-attacks in Estonia in 2007 led to serious re-organisation and changes in cybersecurity practices, not just within Estonia, but across the EU, which led to continuous discussion towards formulating national strategies on cybersecurity for all member-states (Czosseck et al., 2011; Kovács, 2018). Given that small states will continue to fall behind in terms of resource capabilities (compared to bigger states), they should at the very minimum strive to demonstrate their resolve to improve their security culture, rendering them an increasingly more dependable partner. At best, they should re-orient their resources in a way that they prioritise collective security through upgrades of their own security structures.

Assessing conventional security challenges in small states

Conventional types of threats are those that are manifested physically and are widely understood and perceived as direct threats, often related to military action and in the more 'traditional' context of how warfare is conducted via full-scale mobilisation of resources and coercion (Bedeski, 1992, p. 78; Hrnčiar, 2017, pp. 150-151). This may include, *inter alia,* the threat of intervention and/or the direct full-scale military confrontation, prospects of hostile mobilisation and movement closer and around another state's territorial borders and the threat of nuclear proliferation and weapons of mass destruction. Such conventional threats are typically more visible and easily understood. They also have a profound impact on both the target state and society, as they are easily identified as threats that directly impact and endanger people's lives and livelihood (Lee, 2022, p. 155). Small states facing state-driven conventional threats typically perceive them as existential, precisely due to their smallness. The case of Cyprus and Estonia that face conventional threats from Turkey and Russia respectively are indicative examples, as discussed further below.

Small states may exhibit limited capacity to resist external pressure from more powerful states in the material sense (Fox, 1959). If the external threat is manifested as a conventional threat, then, for small states this can be existential, precisely due to their smallness. On the other hand, small states that do not face such external physical pressures, are free from existential threat considerations. Malta, for example, is free from conventional *existential* threats, and does not even have any significant conventional security concerns. On the contrary, Malta is also a neutral EU member-state that does not even take part in the EU's Permanent Structured Cooperation (PESCO): now the only EU member state not to do so. Indeed, strictly speaking participation in PESCO would come into direct conflict with the Maltese constitution (Nováky, 2018, p. 100).

Moreover, the hypothesis that Malta does not face a singular existential threat seems to be corroborated by the opinions of academics and practitioners. In a series of interviews with experts during 2021 and 2022, the opinions on what constitutes a threat varied, while the notion of existential threat was not particularly prominent in the discussions. One senior academic noted climate and rising sea levels as highly significant and not receiving enough attention, especially given the construction underway in coastal areas. Rising sea levels also have a major impact on farming, which leads to the abandon of agricultural practices in Malta (Respondent 21). Other academics highlighted the risk of instability in Libya and the potential for spill-over in Malta. This could be related to specific issues, as was the case with the pilot who deserted and sought refuge in Malta, or to economic repercussions given the significant Maltese investments in Libya, especially in the hotel sector (Respondent 22).

Furthermore, the lack of a single existential threat makes all issues a potential major threat, as Joseph Pisani, Lt Colonel (ret.) in the Armed Forces of Malta, noted. Water resources could be a major threat given that there is heavy dependency on the desalination station, and a major breakdown or an environmental disaster that would contaminate the sea, could become a major concern. Other issues perceived as emerging threats are rather of internal nature, as is the case of the growing population of Malta and the inability of the infrastructure – such as the sewage system – to cope with the increasing needs (Respondent 23). Therefore, with the exception of regional instability and the associated indirect impact on the island, the major threats faced by Malta are either global – for instance, climate change and rising sea levels – or very domestic, such as farming, water shortages, infrastructural deficiencies, and so on. None of them are, however, particularly comparable to the kind of existential external threats faced by the other two cases, and as such the response to these threats differ as well; both in terms of tools and organisation and in terms of scope.

Unlike Malta, Cyprus experiences constant conventional security threats, to the point it has been integrated into the people's routine and lifestyle (Adamides, 2018). Such security threats – in the case of Cyprus, Turkey – are usually the outcome of an overarching existential threat, which is deeply internalised in people's perceptions, routines, and policies (*ibid*.). At the same time, Cyprus experiences non-conventional threats, such as 'greying' of its Exclusive Economic Zone, with daily threats from Turkey in the latter's efforts to control and alter the Republic of Cyprus' jurisdiction in the Eastern Mediterranean (Kontos, 2018; Adamides, 2020, pp. 169-170; Petrikkos, 2022, pp. 91-92)

Similarly in Estonia, the fact that Russia has repeatedly made claims based on cultural, ethnic, and historical pretence instils daily reminders that Russia could hold true to those claims and physically engage Estonia once again (Kennedy-Pipe & Zaidi, 2021, pp. 33-34). Russia, in this sense, could equally be described as an overarching existential threat to Estonia. The difference, however, is that Estonia has more recently experienced unconventional threats from Russia. Yet the latter's looming presence and invasion in Ukraine may have reignited the notion that Russia could equally physically engage other states like Estonia, due to the pre-existing history and embedded trauma of the remnants of Soviet rule (Crandall, 2014; Ploom & Veebel, 2022, p. 71).

How small societies perceive, or even understand, unconventional threats compared to conventional ones may be conditioned by whether they are accustomed to conventional existential threats. In this paper, we argue that states that do not face conventional existential threats are more likely to view hybrid threats as particularly concerning and thus they occupy a central role in their regular security and societal routines. On the other hand, small states that face a conventional (military) existential threat from a superior adversary tend to look at the same or similar hybrid threats through the lens of the actor that poses the existential threat and not necessarily as 'independent security threats'. As a result, other (related or unrelated) threats may be subsumed under the overall existential threat and thus may not receive the attention that they deserve. More importantly, some issues may even be ignored or underestimated if they are not perceived to be linked to the Overarching Existential Threat (OET) (Adamides, 2018). There are at least two issues worth considering if this hypothesis holds: the first is that non-conventional threats cannot necessarily be dealt with via conventional means, and if the unconventional threats are linked to the conventional ones, then the countermeasures, tools, strategies available, as well as the existing 'threat assessment mentality', are unlikely to be particularly efficient. The second has to do with the long-term damage, especially on the societal level, that unconventional threats can inflict on the society because they remain either unrecognised or underappreciated. Either way, opponents of the state can take advantage of these potential shortcomings.

There is also a third scenario that may be of particular importance to the states facing an OET, namely their inability to link seemingly unrelated to the OET threats to the actual OET. Such cases may be part of information operations on seemingly unrelated issues aiming at destabilising the society in a way that makes them less likely to focus on the actual threat. Thus, such destabilising threats may indeed be unrelated to the OET in their essence, but the fact that they oblige societies to allocate time and resources to deal with them, may lead to OET-related issues receiving less attention and resources, with all the risks that this entails.

Formulating security policies: convenience or crude reality and the question of conventional versus unconventional threats

Unconventional threats are frequently less transparent, more complex and less comprehensible than conventional ones. These are threats and tactics that are employed by state and non-state actors, often with technological aids, to deliberately target an opponent and to cause harm for political gain (Bolton, 2021, p. 133; Kennedy-Pipe & Zaidi, 2021, p. 28). Thus, neither the goal or the perpetrator, nor the source of the threat may be readily visible or understood by the targeted society.

In the quest to find an appropriate term that directly captures the essence of hybrid threats and the impact they have on the state, scholars have proposed new terms to describe ongoing processes of warfare and security issues, including 'asymmetry', 'cross-domain coercion', 'hybridity', or even 'next-gen' elements in warfare (Weissmann, 2019; Suchkov,

2019. However, this is not just an academic debate. There is a spill-over effect into the policy making arena, as different measures may be required for different problems. This is evident in works that have addressed the ways through which overly securitising referent objects has led to contested terms and definitions. This is problematic, not just for the state and the policymaker, but also for the rest of society, as specific words used to describe the threats lose their meaning and essentially "everything can be weaponised", because everything could equally be considered a threat (Galeotti, 2022, pp. 9-11).

Bigger states have a tendency to create a very distinct taxonomy of hybrid threats. This is a difficult task for small states, which prefer to either group all threats under one single banner of 'hybridity', or simply distinguish them in terms of either conventional or unconventional types of threats. However, by grouping all hybrid threats together, there is the risk that a state may not find the most suitable response for each kind of hybrid threat, as one size does not fit all. The complexity of finding an appropriate response is linked to the 'ownership' of responsibility in the first place. Unlike the case with conventional threats whereby the responsibility for the response lies with the state, in the unconventional cases the responsibility may lie with the state, the private sector, and/or the society, or may require the contribution of the latter two, depending on the kind of threat. Thus, grouping all unconventional threats as simply 'hybrid' or simply distinguishing between conventional and unconventional is insufficient in formulating the most suitable response to counter such threats.

Definitions, obviously, matter. They do not simply matter in the prevalence of one term over the other in academic debates; definitions matter for the policymaker and the decision-maker who will be implementing measures in countering threats of any kind. While grouping threats under a common banner might be a convenient way of addressing threats holistically, states would also have to develop 'toolboxes' to counter different types of threats. The EU, for instance, has developed a Cyber Toolbox and a Hybrid Toolbox separately. The need for a Hybrid Toolbox was identified under the EU Joint Framework on Countering Hybrid Threats in 2016 and the 2018 Joint Communication aimed at increasing resilience and capabilities against hybrid threats. The toolbox became effective in 2022 and it aims at gathering all civilian and military capabilities and instruments against hybrid threat campaigns, by trickling down four distinct areas to the rest of the member-states, in line with the Joint Framework: (a) *situational awareness*, as part of developing a common strategic culture, (b) *resilience*, to withstand and recover from hybrid attacks, (c) *response*, via diplomatic, crisis-response mechanisms, or restrictive measures, and (d) *cooperation* among the member-states, EU partners, and civil society (European Commission, 2016; Lasoen, 2022). In amassing both civilian and military instruments to further develop a joint response to hybrid threats, member-states would equally benefit, both at an EU level, but also individually.

Typically, hybrid attacks largely concentrate on security infrastructural gaps. Such gaps may include vulnerable day-to-day state and private service areas that people often turn to during their daily routines. At the same time, propagators may also exploit information vulnerabilities to produce misleading information among the civilian population to create tensions and socio-political instability. Such activities may often be connected to the wider cyberspace environment, yet at the same time, they can be recognised as separate and independent attacks. We present three indicative examples of unconventional threats and how each one requires a different kind of response by different kinds of actors: namely, the state alone, state-private sector, and society in general.

(a) National critical infrastructure security: The targeting and directly attacking critical support systems and mechanisms that are vital to the routinely running of the state is detrimental to life and society. Critical infrastructure may include telecommunications, transportation routes and channels, electricity and energy, water supplies, the financial sector, education, and healthcare (Rickli, 2008; Collier and Lackoff, 2020). This is an example where the responsibility for defence lies almost exclusively with the state, be it small or large. So, in essence, the defence approach is very similar to that of conventional threats, even if the tools used for the attack may be unconventional (e.g. cyber-attacks to disrupt the smooth operation of the target).

(b) Cyber-attacks: The cyber capabilities of any country are an integral and essential defence mechanism, especially for those facing an existential conventional threat. This is where Estonia differs significantly to Cyprus and Malta. Much has to do with the former's NATO membership and ability to draw knowledge and resources from the alliance bloc. But it is not just NATO membership that make Estonia stand out in this regard. The small Baltic state also developed a much stronger cyber culture and mentality, and formulated its strategic orientation to focus on the country's cyber capabilities, as opposed to the other two cases that are still much less developed in this regard. Attacks originating in cyberspace that specifically target the apparatus of the state may not differ from those attacks targeting private companies in terms of execution and technical design. However, even if state infrastructure is not the direct target, attacks against significant private companies may still be considered as a national security threat, as they may disrupt the economy and create social unrest, as well as anxiety that the government is unable to protect its citizens. Thus, in this case there is a need for state-private sector collaboration as the state cannot prevent attacks against the private sector, but it still has the responsibility to maintain an uninterrupted and healthy economic and societal environment. The issue with small states is that some private companies, especially in the finance sector, may be integral to the functioning of the country's economic environment. An indicative example is the Bank of Valletta (BOV) cyber-attack incident of 2019, where BOV, being responsible for a significant share of Malta's financial activities, fell victim to such attacks (Vella, 2019).

(c) Information operations: These refer to tactics and functions that deliberately manipulate information. This may also include diplomatic tactics that utilise public and digital tools of diplomacy, to uplift, legitimise or positively reinforce through the power of narratives the initiating entity. At the same time, these operations can intentionally target an opponent to negatively affect their image and the societal fabric exploiting already existing societal divisions. Often such operations are carried out through 'disinformation' campaigns; a type of unconventional threat initiated by a hostile entity to target an adversary with the sole purpose of misguiding and confusing target audiences, either within the target's country or other close allies who retain good and/or friendly relations with the target in question. Oftentimes, disinformation tactics may coincide with cyber-attacks, as highlighted in scholarship and in practice, including the Maltese Ministry for Foreign and European Affairs (Schmidt, 2014, p. 74; Farrugia, 2020). Provided that it is practically impossible to prevent information campaigns, societies are required to become more resilient to such attacks. As discussed later, in this regard the resilience of small states may be different compared to bigger ones, precisely due to their size.

It should be noted that IT/cyber-related operations do indeed occupy a big portion of the hybrid arena in contemporary conflicts. While we acknowledge this, the goal in this paper is to examine how the small EU states under consideration respond to unconventional threats in general. In this sense, and as argued elsewhere (Daniel & Eberle, 2018; Danyk et al., 2017;

Kalniete & Pildegovičs, 2021), we too acknowledge that 'cyber' is often conceptualised and included as a component under the wider 'hybrid threats/warfare' umbrella. Under the EU Joint Framework on Countering Hybrid Threats, all three cases employ National Computer Security Incidence Response Teams (CSIRTs) that primarily deal with cyber threats. The growing nature of hybrid and unconventional threats, however, has pushed such Teams to address other threats as well, including information-related threats – by educating the civilian population on combating disinformation – and critical security infrastructure that affects not just the state's critical operations, but also the society at large (Giumelli et al., 2018, pp. 147-149).

The case of Estonia is once again different compared to the other two cases; it maintains considerable advantages, not least infrastructurally, governance-wise, or in terms of capabilities, as compared to the cases of Cyprus and Malta. The latter two have merely accelerated their cyber capabilities in recent years, and more notably following the breakout of the COVID-19 pandemic, while their cyber-security strategies at the moment of writing being under revision, and not yet finalised. The first Cypriot National Cybersecurity Strategy was initially presented via the ENISA Directive in 2012; although the actual deliverable and the Strategy itself was published only in 2020, right before the pandemic. Similarly, the Maltese strategy was first published in 2016. The Estonia's Cybersecurity Strategy of 2019-2022 is also currently under review, yet its execution throughout its marked period enabled flexibility in dealing with the pandemic (Respondent 8). Furthermore, Estonia's relationship with NATO, as well as the state's strategic communications, have both enhanced the way Estonian e-governance and cybersecurity practices are portrayed within the EU and in the rest of the world. This has normalised Estonia's portrayal as a pioneer and entrepreneur when it comes to cyber and e-governance (Adamson, 2019). Whether these notable capabilities act as a major deterring factor remains to be seen. In any case, Estonia's infrastructure paves the way for Estonia as a small state with a niche in e-governance and cyber security, which could pose as a model for small and bigger states alike to follow.

Policy overlaps: Foreign, defence and security

Unlike the response and deterrence to conventional threats – which is primarily the responsibility of the armed forces and the Ministry of Defence (MoD) – resilience, deterrence and defence against unconventional threats has become the responsibility of all government sectors, as well as that of the private sector and society at large (Major & Mölling, 2015; Wilkinson, 2020). This section focuses specifically on the overlap of the ministries of defence and foreign affairs in small states and how they often need to coordinate and complement their activities to maximise the country's defensive options, given their limited accessibility to resources. Defence diplomacy, a concern and traditional goal of mostly great powers, has now become an integral part of the ministries of defence of small and medium sized states as well, with inevitably different goals due to size limitations. This is primarily the outcome of the growing presence of more hybrid and more extra-regional threats, such as cyber-attacks, terrorism, and information operations (Rogers, 2018) as well as grey-zone operations that range economic subversion to the questioning of sovereignty and jurisdiction, to geopolitical gaslighting. Such threats require more international cooperation, and subsequently the need for more diplomacy in the security and defence sector. International cooperation against such threats relies heavily on shared intelligence and even collective resilience, since a small state may create disproportionately serious problems if it becomes the weakest link in the bloc to which it belongs (Respondent 9; Respondent 13; Respondent 17).

More international cooperation and intelligence sharing relies on more diplomacy-oriented inter and intra-governmental practices, which in turn, requires changes in the traditional MoD Standard Operating Procedures (SOPs), which include closer collaboration with the Ministry of Foreign Affairs (MFA). We should note at this point that these intra-governmental practices apply to countries that have a Ministry of Defence in the 'traditional sense' as is the case of Cyprus and Estonia (Respondent 18). This does not apply to Malta, which does not have a distinct ministry for defence (Respondent 19).

This closer intra-governmental cooperation may also entail assigning MFA staff to the MoD as liaisons who bridge and complement each Ministry's needs, or in some cases even conflate the defence responsibilities with the diplomatic ones under the same ministry (Respondent 10; Respondent 14). This is especially the case where the primary coordination for the security lies with the MFA, as is the case with Cyprus. Consequently, the MFA works closely with other ministries and entities for the provision of security clearances, authorising training missions within the context of the Common Security and Defence Policy and in liaison with the MoD while, at the same time, providing useful information to the Commissioner for Communications and the CSIRT that monitors security information, alongside the intelligence services (Respondent 12; Respondent 20). The reverse may be true if the MoD has the primary responsibility, as is the case with Estonia. Similarly, other small states conflate the responsibilities of security, diplomacy and home affairs. In Malta, the Defence Matters Directorate is part of the Office of the Prime Minister (OPM) and aims to 'consolidate and develop the defence function of the OPM' and liaises with the MFA for the purpose of bilateral and multilateral defence relations (Government of Malta, Ministry for Foreign and European Affairs, 2022; Republic of Malta, Ministry of Home Affairs). This shows that defence and security matters are jointly coordinated by state entities in the same manner as observed in Cyprus and Estonia. Therefore, central resource allocation enables existing functions for addressing security and defence needs in these three small states.

International MoD and national guard activities are more frequently incorporated in the mainstream diplomatic arena and are 'exposed' to the public eye, concurrently highlighting the level of bilateral or multilateral relationship status among the states involved (Respondent 15; Respondent 16). The goal is not just to enhance collaborations on defence-related matters, but also to strengthen the overall diplomatic status and public perceptions, in a way that would ultimately also allow for deeper multi-level security-related relations (Gilboa, 2008; Iaydjiev, 2011; Respondent 11; Respondent 14). Thus, such activities are part of information operations. Domestically, these activities are usually portrayed as positive and security-enhancing, but in cases where there are zero-sum mentality environments due to conflicts or internalised perceptions, as it is in the case of Cyprus, such actions are usually denigrated by the opposing side of the conflict as negative, dangerous, destabilising and ultimately not helpful towards conflict resolution (Adamides, 2020).

While for small states such collaboration and the subsequent information campaigns are key in their attempt to balance against threats and to upgrade their value, there is also the question of the actual capabilities and resources required to efficiently focus on security matters related to unconventional threats. It is not just the expected lack of resources, human capital and expertise that small states may lack compared to bigger ones; it is also the lack of experience and the mentality, or culture, to deal with such threats. The latter is an issue that is frequently acknowledged by the responsible civil servants. There has certainly been improvement in terms of training and expertise, especially on the cyber front, but not necessarily on other forms of hybrid threats, especially regarding information operations. While small states are enhancing their capabilities of defending their critical infrastructure against cyber-attacks – primarily through the CSIRT actions – the same cannot be said about their ability to closely monitor and efficiently handle information operations. As mentioned, the risk is both to the state itself as well as to allies and other political and security partners, if an ill-prepared country becomes the weakest link in an interlinked security environment.

Despite the risks mentioned above, small states may have some inherent advantages compared to bigger, more populous, and diverse countries. Specifically, given their smallness, they can work on their weaknesses relatively quickly once identified, especially if they have the assistance of more experienced partners. Simultaneously, a small society may be more resilient to information operations, even though the reverse may be also true in some circumstances; namely falsehoods may spread to the entire society quite rapidly. Lastly, given the absence of resources to tackle all potential hybrid threats, a small state may be forced to focus on developing closer regional and bilateral security relations with much stronger players. However, since security is never free, the small state must find ways to 'pay' for the services of the provider and towards this end new mutually beneficial collaborations may emerge that may have substantial spill-over effects with much more significant *long-term* political benefits. The cases of Cyprus, Estonia and Malta are witness to such possibilities.

Diplomacy-military connection: the Eastern Mediterranean case

The EastMed defence relations that transpose into diplomatic ones are indicative examples of the aforementioned arguments. Common regional military drills with the presence of forces from Cyprus, Greece, Israel, Egypt, and Jordan, as well as the frequent arrival of the Charles de Gaulle aircraft carrier (among others) in the port city of Limassol in Cyprus receive particular attention in and out of the diplomatic circles. Inevitably, military collaborations also receive particular attention in the media and are frequently portrayed as evidence of a deepening and broadening of bilateral and multilateral regional relations by political elites. The soft power-driven diplomacy of powerful states like France and the US, and the subsequent spill-over effects in the Cypriot society, are also manifested and promoted through social events when their warships dock in Cyprus. Indeed, during such visits, political, societal, military, and academic 'elites' are repeatedly invited as part of networking and defence diplomacy initiatives, frequently leading to subsequent collaborations in the respective fields of the visitors. From a positively oriented information perspective, the specific events do not just receive 'official' attention, but also unofficial exposure in social media by many participants and their respective networks, thus also contributing to changing societal perceptions regarding the specific countries. This is particularly notable in the case of the US, which traditionally was not well-perceived among and by the Greek-Cypriot community (Adamides, 2014).

There is a reason why Cyprus chooses to emphasise such activities. The first, and frequently the only realistic, line of defence for small states – especially the ones that are under an existential threat from a militarily superior adversary – is diplomacy. The second is balancing by upgrading their (small state's) value for stronger and influential actors who could potentially offer some form of protection by keeping the potential aggressor at bay. The two are frequently well-connected as it is a question of perception, public acceptance, and ultimately a variable of soft power (Thorhallsson, 2019, pp. 380, 385-386). An additional level of defence takes place through 'sheltering', whereby large organisations and blocs such as the EU could provide an additional level protection to small states. EU accession was seen as an ideal 'shelter' against the ongoing dispute and the daily threat of Turkey. Indeed, as Ioannis Kasoulides, the Cypriot former Minister of Foreign Affairs, noted, accession to the EU 'is the greatest guarantee of our existence' (Adamides, 2018, p. 77). Cyprus does not just see the EU as a shelter though; it also sees it as an arena in which it has the ability, by adopting different measures discussed at EU level, to elevate itself among its peers, showing its commitment and being a responsible member-state towards broader EU security and defence-related policies.

Small states may also seek shelter through bilateral relations, and the Republic of Cyprus (RoC) is not an exception. However, the public perceptions have contributed to the development of a 'selective' strategy, not least due to historical taboos and considerations regarding political balancing between major powers such as the US and Russia. Indeed, collaboration with the US was taboo if not completely unacceptable, as the latter is frequently blamed for many of the problems the RoC faces with Turkey (Adamides, 2014). However, partly due to the aforementioned defence diplomacy activities, and partly due to the deteriorating relations between the US and Turkey on one hand, and between Cyprus and Russia on the other due to the war in Ukraine, Cyprus has gained (relative) value for the US and more Cypriots welcome the collaborations, and overall, the heavier US footprint in Cyprus. A good example of this change is the Cyprus Center for Land, Open-seas and Port Security (CyCLOPS), a highly specialised training centre partly funded by the US and frequently featured at the US Embassy in Cyprus (US Embassy Nicosia, 2020). Furthermore, in recent opinion polls following the Russian invasion of Ukraine, 73% of Greek Cypriots would welcome NATO membership (Simerini 2022). These developments and shifts in public perceptions are a success story for the MoD as much as they are for the MFA.

Even the case of the British Sovereign Base Areas, which has been a very contested issue for the RoC, is being reconceptualised. The degree of collaboration between the government and the SBA could indeed indicate and signal a change in the way of dealing with common security concerns. We currently observe an increasingly collaborative framework between RoC and Britain, despite Brexit. Concurrently, the issue of the SBA seem to be on a desecuritising path, whereby elite and public do not consider the Bases as a political and security priority for RoC. As such, the presence of the SBA in public political discussions has been reduced substantially, and when it does appear in discussions, it is now rarely discussed in negative terms, compared to previous years which was almost always presented as negative.

Similarly, in the case of Estonia, the diplomacy-military connection nexus is particularly distinct and important to the state. Defence attachés are required to be positioned together with MFA diplomats when furthering Estonian military and defence interests abroad, especially within major decision-making bodies in Brussels (Respondent 8; Respondent 4). Similarly, the Estonian-based NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE) is a key instrument that enhances Estonian defence diplomacy through research, coordinated activities and planning with other EU member states. Widely seen as NATO's cyber-defence hub, the CCDCoE is also involved in hosting and organising large-scale events such as the International Conference on Cyber Conflict that bridges academia and practitioners over related subjects on hybrid warfare and cyber-security at the local, regional, and international levels (Respondent 1; Respondent 7).

The Estonian connection to NATO runs deep, primarily due to how Estonian security and defence is structured. Estonian defence structures, including the Estonian Defence Force, have adopted NATO language and tactics in matters concerning defence capabilities and planning (Veebel et al., 2020, p. 17), as well as territoriality and space, and other material resources employed for the purpose of defence against conventional threats. Noteworthy here is the distinction between security and defence: defence is provided by NATO (Council of the European Union, 2022) since it has been argued that the CSDP itself is not enough for the security of the Baltic states (Gladysh, 2016). NATO as a defence provider is the primary 'destination' for countries like Estonia in case of crises, not least because practices related to the CSDP "should not compete with, undermine, or duplicate NATO" (Raik & Šešelgyte, 2022, p. 283). Security itself, on the other hand, incorporates more CSDP structures: this provides a framework that addresses unconventional threats. Nonetheless, the paradoxical nature of responding to unconventional threats that have physical implications (so as to cause harm to civilians) such as terrorism, also implies that NATO is still involved in countering such threats (Demetriou, 2016). This means that, while CSDP frames and conceptualises such threats, NATO remains the executive force that counters threats. This distinction is upheld by Estonia when conceptualising security and defence policy (Raik & Rikmann, 2021, p. 612). By maintaining the security-defence distinction and unlike Cyprus and Malta, that are non-NATO members, Estonia has prioritised NATO defence structures over EU defence structures.

The fact that Estonia has the capacity to organise such large-scale events and coordinate responses to cyber-related issues is the product of the 2007 cyber-attacks on Estonia (Traynor, 2007; The Economist, 2010; Respondent 2; Respondent 3). The 2007 attacks also became a distinct conversation point within the EU: it was the first time an EU member-state was exposed to significant risk and potential financial ruin due to an unconventional attack of such magnitude. It became very clear that financial stability across the EU had to be protected. The first step was to trace vulnerability gaps found in other member-states, as it was the case of Estonia, where the state's critical infrastructure and societal fabric suffered in the aftermath of the attacks. Therefore, as a small state, Estonia had to further prioritise cybersecurity-related areas, in order to increase resilience and to overcome any other future attacks. The state has, in fact, managed to considerably uplift itself in designing a more resilient e-governance and cybersecurity infrastructure that brings together other EU and NATO member states on issues related to cyber-defence, thus establishing a clear diplomacy-military connection, as well as an image of a small yet very powerful state in this security domain (Respondent 5; Respondent 6; Respondent 7). Moreover, as explained by an Estonian Ministry of Defence official at the Cyber Defence Policy department (Respondent 8), Estonian cyber defence policy integrates all unconventional types of security issues and often views them collectively as part of the 'hybrid threat' nexus, while at the same time, current cyber defence and deterrence policy is considered a national defence strategy and priority, as outlined in the 2019-2022 strategy document. Therefore, policy as such is not solely a matter of defence alone, but rather an integral part of several stakeholders, including the Estonian Ministry of Foreign Affairs (Pernik, 2021, p. 11; Ministry of Defence of the Republic of Estonia, 2017; Respondent 4; Respondent 5).

In the case of Malta, the Ministry for Foreign & European Affairs is pivotal in coordinating policy both in foreign affairs, as well as domestically wherever foreign policy is concerned. The Maltese MFA, thus, can link issues of security and defence at home and beyond, with particular reference to the EU itself (Respondent 19; Respondent 21). This is also highlighted in the identity of the Ministry, with its name highlighting the Ministry's focus on both foreign and European relations (Republic of Malta, Ministry of Home Affairs n.d.; Government of Malta, Ministry for Foreign and European Affairs, 2022, pp. 10, 13). As a small island state, Malta is an active and enthusiastic participant on EU foreign and security policy matters. Malta lacks a pertinent MoD, defence forces or defence diplomats; but the Armed Forces of Malta (AFM) collaborate with other governments (e.g. with Italy) and within the EU over matters of search and rescue; these operations become part of a wider strategy that can involve pushbacks and placing migrants at detention centres (DeBattista, 2016, p. 73). Such policy formulation, which aims at preventing migrants from reaching the EU mainland, has been the product of overly securitised borders, triggered by EU migration policy (Lemaire, 2019, p. 718). Thus, there is a specific security need at EU level, which Malta cannot fully fulfil, not least due to its limited resources, as well as its neutral strategic posture. Indeed, the limited role of the Maltese AFM in search and rescue operations at sea sees Malta often exiting the negotiations room during classified discussions on defence (DeBattista, 2016, p. 80).

Conclusion

The three cases shed some light on how small states tend to assess their foreign, defence and security priorities, often in an overlapping manner. This overlap may mean that policy across these fields becomes so interconnected in terms of application that it becomes particularly challenging to exercise policy without coordinating, facilitating and engaging all foreign, defence and security-related sectors. Irrespective of how each small state coordinates and links its processes internally across its state agencies, there are at least three common variables in most small states (and certainly in the ones we examined) worth highlighting; these have a major impact on small states' security identity and role, and on how they can handle hybrid threats.

One of the primary issues is that of *understaffing*. This is one resource limitation that is most noticeable across all departments involved with security, defence and foreign policy. This matters because small states cannot rely on their own materiality alone and thus need to develop additional capabilities to fulfil a policy-oriented agenda (Ehrhardt & Oliver, 2007). In doing so, however, they must reallocate resources and time that would have been otherwise used elsewhere, in other policy priorities. Therefore, to minimise the impact, small states may overburden their agents and officers in taking up relevant responsibilities in addition to their existing duties. This could lead to either inefficient actions due to lack of expertise, or significant gaps due to lack of implementation capacity (time and resources).

Furthermore, hybrid threats tend to be grouped together and/or broken into groups of conventional and unconventional types of threats with the risks that are examined above. While it might be convenient in terms of producing a faster response, there is a high risk that policy formulation by 'grouping' might be problematic and erroneous, particularly because the grouping of threats as such could lead to skewed responses. Instead, the contested nature of hybrid threats and the lack of consensus in policy and academic circles constitutes a Wicked Problem of joined-up threats, which in turn require joined-up responses (Zaidi, 2019; Rittle & Weber, 1973). In this dichotomy of conventional and unconventional threats, it is also useful to remember the distinction between states that face conventional existential threats and those that do not. The former are more likely to include the unconventional threats under the OET umbrella, frequently ignoring or under-estimating potential threats that do not 'fit' the OET framework. Similarly, the focus and the associated mentality may be on conventional defence tools and operations, often allowing 'gaps' for unconventional threats to materialise and fester.

The aforementioned issues pose security challenges to small states. Small states must not just seek ways to build resilience and defence mechanisms against a growing number of unconventional and increasingly complex threats, but also develop or maintain their status as reliable security partners. Indeed, the need for more international collaboration and shared intelligence to counter unconventional threats is, or should, always be juxtaposed to the risk of becoming the weakest link in the bloc's 'security chain'. Despite their obvious limitations, small states, under certain conditions – usually subject to proper infrastructure, training, education, and frame of mind (security and defence culture) – can potentially 'punch above their weight' and become a disproportionately significant player in countering unconventional threats. This is highly unlikely in the conventional security arena, given the inherent limitations that small states have in terms of size, population, economic power and, of course, military forces; but this does not necessarily apply to unconventional threats.

Annex: Interviews

Interviews

Respondent 1 Dr Matthew Crandall, (Associate Professor, School of Governance, Law and Society, Tallinn University) [26 April 2021 and 20 September 2021]

Respondent 2 Dr Veiko Lember (Senior Research, Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology) [21 September 2021]

Respondent 3 Dr Külli Sarapuu (Associate Professor, Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology) [21 September 2021]

Respondent 4 Dr Kristi Raik (Director, Foreign Policy Institute, International Centre for Defence and Security, Tallinn) [2 June 2021 and 22 September 2021]

Respondent 5 Professor Robert Krimmer (Former ERA-Chair of e-Governance, Skytte Institute, University of Tartu) [20 May 2021 and 23 September 2021]

Respondent 6 Dr Mihkel Solvak (Associate Professor, Johan Skytte Institute of Political Studies, University of Tartu) [23 September 2021]

Respondent 7 Annela Kiirats (Officer, e-Governance Academy, Estonia) [24 September 2021]

Respondent 8 Cyber Policy Unit Officer (Ministry of Defence of the Republic of Estonia) [6 May 2021]

Respondent 9 LT Colonel Symeon Zambas (President of European Citizens Association; Director of the Security and Defence Academy, Ministry of Defence of the Republic of Cyprus) [5 May 2022]

Respondent 10 Attaché A, Security Policy Department, Ministry of Foreign Affairs of the Republic of Cyprus) [30 May 2022]

Respondent 11 Attaché B, Security Policy Department, Ministry of Foreign Affairs of the Republic of Cyprus) [30 May 2022]

Respondent 12 Officer, Cyber Security Incident Response Team – CSIRT (Digital Security Authority, Office of the Commissioner of Communications, Republic of Cyprus) [2 June 2022]

Respondent 13 Security Officer, Security Services of the Republic of Cyprus [14 April 2022]

Respondent 14 Attaché C, Ministry of Foreign Affairs, Republic of Cyprus) [31 May 2022]

Respondent 15 Thessalia Salina Shambos (Director, Middle East, Gulf and Africa, Ministry of Foreign Affairs of the Republic of Cyprus) [6 June 2022]

Respondent 16 Colonel Dr Harald Gell (Associate Professor, Theresan Military Academy, Austria; Chairman of the Military Erasmus – EMILYO) [5 May 2022]

Respondent 17 Military Attaché (Permanent Representation of the Republic of Cyprus to the European Union) [11 July 2022]

Respondent 18 Military Officer (National Security Agency, Ministry of Defence of the Republic of Cyprus) [21 July 2022]

Respondent 19 Malta Expert and Academic [8 August 2022]

Respondent 20 CSIRT Officers (Digital Security Authority, Office of the Commissioner of Communications, Republic of Cyprus) [20 October 2022]

Respondent 21 Senior Academic, University of Malta [15 December 2022]

Respondent 22 Dr. Monika Wohlfeld, German Chair for Peace Studies and Conflict Prevention, (Mediterranean Academy of Diplomatic Studies – MEDAC, University of Malta) [16 December 2022]

Respondent 23 Lt Colonel (ret.) Joseph Pisani, (International Affairs Branch, Armed Forces of Malta) [17 December 2022].

Disclaimer

This paper did not benefit from research funding. The authors do not identify any conflicts of interest.

References

Adamides, C. (2014). Negative perceptions of foreign actors: An integral part of conflict perpetuating routines. In M. Kontos, N. Panayiotides, H. Alexandrou, & S. Theodoulou (Eds.), *Great power politics in Cyprus: Foreign interventions and domestic perceptions* (pp. 197-222). Newcastle: Cambridge Scholar Publishing.

Adamides, C. (2018). The challenge of formulating National Security Strategies (NSS) in the presence of overarching existential threats. *Cyprus Review*, *30*(1), 71-94.

Adamides, C. (2020). *Securitization and desecuritization processes in protracted conflicts: The case of Cyprus*. Cham: Springer International Publishing.

Adamson, L. (2019). Let them roar: Small states as cyber norm entrepreneurs. *European Foreign Affairs Review*, *24*(2), 217-234.

Alford, J. (1984). Security dilemmas of small states. *The Round Table: Commonwealth Journal of International Affairs*, *73*(292), 377-382.

Archer, C., Bailes, A. J. K., and Wivel, A. (Eds.) (2014). *Small states and international security: Europe and beyond*. London: Routledge.

Bailes, A. J. K., Rickli, J., and Thorhallsson, B. (2014). Small states, survival and strategy. In C. Archer, A.J.K. Bailes & A. Wivel, A. (Eds.), *Small states and international security: Europe and beyond* (pp. 26-45). London: Routledge.

Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, *19*(1), 62-70.

Baldacchino, G. and Wivel, A. (2020). Small states: Concepts and theories. In G. Baldacchino & A. Wivel (Eds.), *Handbook on the politics of small states* (pp. 1-19), Cheltenham: Edward Elgar.

Barston, R. P. (1973). *The other powers: Studies in the foreign policies of small states*. London: Allen & Unwin.

Bedeski, R. E. (1992). Unconventional security threats - an overview. *Interdisciplinary Peace Research,* Formerly *Pacifica Review: Peace, Security & Global Change*, *4*(2), 78-90.

Bolton, D. (2021). Targeting ontological security: Information warfare in the modern age. *Political Psychology*, *42*(1), 127-142.

Bressan, S., and Sulg, M. (2020). Welcome to the grey zone: Future war and peace. *New Perspectives*, *28*(3), 379-397.

Collier, S.J. and Lackoff, A. (2020). The vulnerability of vital systems: How 'critical infrastructure' became a security problem. In M Cavelty & K. Kristensen (Eds.), *Securing 'the homeland': Critical infrastructure, risk and (in)security* (pp. 17-39). London: Routledge.

Council of the European Union (2022). *A strategic compass for security and defence*. Brussels: Council of the European Union.

Crandall, M. (2014). Soft security threats and small states: The case of Estonia. *Defence Studies*, *14*(1), 30-55.

Czosseck, C., Ottis, R., and Talihärm, A. M. (2011). Estonia after the 2007 cyber-attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism, 1*(1), 24-34.

Daniel, J. and Eberle, J. (2018). Hybrid warriors: Transforming Czech security through the 'Russian hybrid warfare' assemblage. *Sociologický časopis / Czech Sociological Review, 54*(6), 907-931.

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. *Connections, 16*(2), 5-24.

DeBattista, A. P. (2016). A small-island state within a changing security climate: The case of Malta. *Symposium Melitensia*, *12*(1), 69-86.

Demetriou, P. (2016). NATO & CSDP: Can the EU afford to go solo? *Cogent Social Sciences, 2(1)*, 1208376.

Ehrhardt, D. and Oliver, C. (2007). *Big challenges, small states: Regulatory options to overcome infrastructure constraints*. Washington, DC: The World Bank.

European Commission (2016). *Joint Framework on countering hybrid threats: A European Union response*. Brussels: JOIN(2016).

Farrugia, D. (2020). Hybrid threats and disinformation: The COVID-19 pandemic. https://foreign.gov.mt/en/perspectives-on-the-work-of-the-ministry/pages/hybrid-threats-and-disinformation-the-covid-19-pandemic.aspx

Fox, A. B. (1959). *The power of small states: Diplomacy in World War II*. Chicago, IL: The University of Chicago Press.

Galeotti, M. (2022). *The Weaponisation of everything: A field guide to the new way of war*. New Haven, CT: Yale University Press.

Galinec, D., Steingartner, W., and Zebić, V. (2019). Cyber rapid response team: An option within hybrid threats. In *IEEE 15th International Scientific Conference on Informatics* (pp. 43-50). IEEE.

Gilboa, E. (2008). Searching for a theory of public diplomacy. *The Annals of the American Academy of Political and Social Science*, *616*(1), 55-77.

Giumelli, F., Cusumano, E., & Besana, M. (2018). From strategic communication to Sanctions: The European Union's approach to hybrid threats. In E. Cusumano & M. Corbe (Eds.), *A civil-military response to hybrid threats* (pp. 145-197). Cham: Palgrave Macmillan.

Gladysh, M. (2016). Security of the Baltic states: Effectiveness of the EU Common Security and Defence Policy and influence of the Ukrainian crisis. *Przegląd Politologiczny (Political Science Review), 3/2016*, 187-198.

Goetschel, L. (1998). The foreign and security policy interests of small states in today's Europe. In *Small states inside and outside the European Union* (pp. 13-31). Boston MA: Springer.

Government of Malta Ministry for Foreign and European Affairs (2022). *Malta's foreign policy strategy*. Valletta: Government of the Republic of Malta.

Hom, A. R. and Steele, B. J. (2020). Anxiety, time, and ontological security's third-image potential. *International Theory*, *12*(2), 322-336.

Hrnčiar, M. (2017). Keystones of irregular warfare. *International Conference Knowledge-Based Organization*, *23*(1), 150-154.

Hughes, G. (2020). War in the grey zone: Historical reflections and contemporary implications. *Survival*, *62*(3), 131-158.

Iaydjiev, I. (2011). Searching for influence and persuasion in network-oriented public diplomacy: What role for 'small states'? *Exchange: The Journal of Public Diplomacy*, *2*(1), 40-48.

Ingebritsen, C., Neumann, I. B., Gstöhl, S., and Beyer, J. (2006). *Small states in international relations*. Seattle, WA and Reykjavik: University of Washington Press and University of Iceland Press.

Kalniete, S. and Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. *European View*, *20*(1), 23-33.

Kennedy-Pipe, C. and Zaidi, I. (2021). The hybrid challenge and small states. In A.-M. Brady & B. Thorhallsson (Eds.), *Small states and the new security environment* (pp. 27-39). Cham: Springer.

Keohane, Robert O. (1969). Lilliputians' dilemmas: Small states in international politics. *International Organization*, *23*(2), 291-310.

Kontos, M. (2018). Power games in the exclusive economic zone of the Republic of Cyprus: The trouble with Turkey's coercive diplomacy. *Cyprus Review, 30*(1), 51-70.

Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO, *Land Forces Academy Review, 23*(1), 16-24.

Lamoreaux, J. W. and Galbreath, D. J. (2008). The Baltic states as 'small states': Negotiating the 'East' by engaging the 'West'. *Journal of Baltic Studies, 39*(1), 1-14.

Lasoen, K. (2022). Realising the EU hybrid toolbox: opportunities and pitfalls. Policy Brief. The Hague: Clingendael – The Netherlands Institute of International Relations.

Lee, S. (2022). Towards instability: the shifting nuclear conventional dynamics in the Taiwan Strait. *Journal for Peace and Nuclear Disarmament*, *5*(S1), 154-166.

Lemaire, L. (2019). The European dispositif of border control in Malta. Migrants' experiences of a securitized borderland, *Journal of Borderlands Studies*, *34*(5), 717-732.

Major, C. and Mölling, C. (2015). *A hybrid security policy for Europe: resilience, deterrence, and defence as leitmotifs*. No. 22/2015 (SWP Comments), Berlin: SWP.

Ministry of Defence of the Republic of Estonia (2017). *National security concept of Estonia*, Tallinn: Ministry of Defence of the Republic of Estonia.

Ministry of Foreign Affairs (MFA) of the Republic of Cyprus (2022). https://mfa.gov.cy/mission,-organisation-and-finances/

Neumann, I. B. and de Carvalho, B. (2015). Introduction: Small states and status. In B. de Carvalho & I. B. Neumann (Eds.), *Small state status seeking* (pp. 1-21). New York: Routledge.

Nováky, N. (2018). The EU's permanent structured cooperation in defence: Keeping sleeping beauty from snoozing. *European View*, *17*(1), 97-104.

Pernik, P. (2021). *Cyber deterrence: A case study on Estonia's policies and practice*. Hybrid CoE Paper 8. Helsinki: European Centre of Excellence for Countering Hybrid Threats.

Petrikkos, P. (2022). Stuck in the middle: Constructing maturity and restoring balance in RoC-EU Relations. In Z. Tziarras (Ed.), *The foreign policy of the Republic of Cyprus: Local, regional and international dimensions* (pp. 77-104), Cham: Palgrave Macmillan.

Ploom, I. and Veebel, V. (2022). Estonia: the increased focus on geopolitics after Russia's invasion of Ukraine. In A. Sprūds & M. Vargulis (Eds.), *Three seas initiative: mapping national perspectives* (pp. 71-80), Riga: Latvian Institute of International Affairs.

Raik, K. and Rikmann, E. (2021). Resisting domestic and external pressure towards de-Europeanization of foreign policy? The case of Estonia. *Journal of European Integration, 43(5),* 603-618.

Raik, K. and Šešelgyte, M. (2022). Estonia, Latvia and Lithuania. In T. Tardy (Ed.), *The nations of NATO: Shaping the Alliance's relevance and cohesion* (pp. 279-299). Oxford: Oxford University Press.

Rehrl, J, (Ed.). (2021). *Handbook on CSDP: The Common Security and Defence Policy of the European Union*. Vienna: Federal Ministry of Defence of the Republic of Austria.

Republic of Malta Ministry of Home Affairs (n.d.). Defence Matters Directorate. https://homeaffairs.gov.mt/en/MHAS-Departments/Defence%20Matters%20Directorate/Pages/Defence-Matters-Directorate.aspx

Rickli, J. (2008). European small states' military policies after the Cold War: from territorial to niche strategies, *Cambridge Review of International Affairs*, *21*(3), 307-325.

Rogers, J. (2018). Reinforcing deterrence through societal resilience: countering hybrid threats in the Baltic region. In E. Cusumano & M. Corbe (Eds.) *A civil-military response to hybrid threats* (pp. 259-280), Cham: Palgrave Macmillan.

Rumelili, B. (2015). *Conflict resolution and ontological security: peace anxieties*. New York: Routledge.

Sovereign Base Areas Administration (SBAA) (n.d.). Civil Administration (Area Offices) Akrotiri / Dhekelia, SBAA. https://www.sbaadministration.org/

Schmidt, N. (2014). Neither conventional war, nor a cyber war, but a long-lasting and silent hybrid war, *Obrana a Strategie*, *14*(2), 73-86.

Simerini (2022). Δημοσκόπηση:Ένταξη της Κύπρου στο ΝΑΤΟ προκρίνουν οι Πολίτες. [Opinion poll: Citizens want Cyprus accession to NATO]. https://simerini.sigmalive.com/article/2022/10/9/demoskopese-entaxe-tes-kuprou-sto-nato-prokrinoun-oi-polites/

Steele, B. J. (2008). *Ontological security in International Relations: Self-identity and the IR state*. London: Routledge.

Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military and political practice. *Small Wars & Insurgencies*, *32*(3), 415-440.

The Economist (2010). War in the fifth domain. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

Thorhallsson, B. (2018). Studying small states: A review. *Small States & Territories*, *1*(1), 17-34.

Thorhallsson, B. (2019). Small states and the changing global order: what small state theory c can offer New Zealand foreign policymaking. In A. Brady (Ed.) *Small states and the changing global order* (pp. 379-395). Cham: Springer.

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., and McCue, M. (2018). *Addressing hybrid threats*, Stockholm: Swedish Defence University.

US Embassy Nicosia (2020). The Cyprus Center for Land, Open Seas, and Port Security, https://cy.usembassy.gov/the-cyprus-center-for-land-open-seas-and-port-security/

Vaicekauskaitė, Ž. M. (2017). Security strategies of small states in a changing world, *Journal of Baltic Security*, *3*(2), 7-15.

Veebel, V., Ploom, I., Vihmand, L., and Zaleski, K. (2020). Territorial defence, comprehensive defence and total defence: Meanings and differences in the Estonian Defence Force, *Journal of Baltic Security, 6(2)*, 17-29.

Vella, M. (2021). BOV cyber-heist: Canadian money launderer pleads guilty. https://www.maltatoday.com.mt/news/court_and_police/112001/bov_cyberheist_canadian_money_launderer_pleads_guilty#.Y2N9_nZBy01

Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework, *Journal of Baltic Studies*, *5*(1), 17-26.

Wilkinson, E. (2020). Resilience and deterrence: exploring correspondence between the concepts. In A. Filippidou (Ed.), *Deterrence: Concepts and approaches for current and emerging threats* (pp. 19-33). Cham: Springer.

Zaidi, I. (2019). Hybrid challenge: Whose problem is it anyway?. In *Pakistan Army Green Book* (pp. 10-29). Rawalpindi: IGT&E.