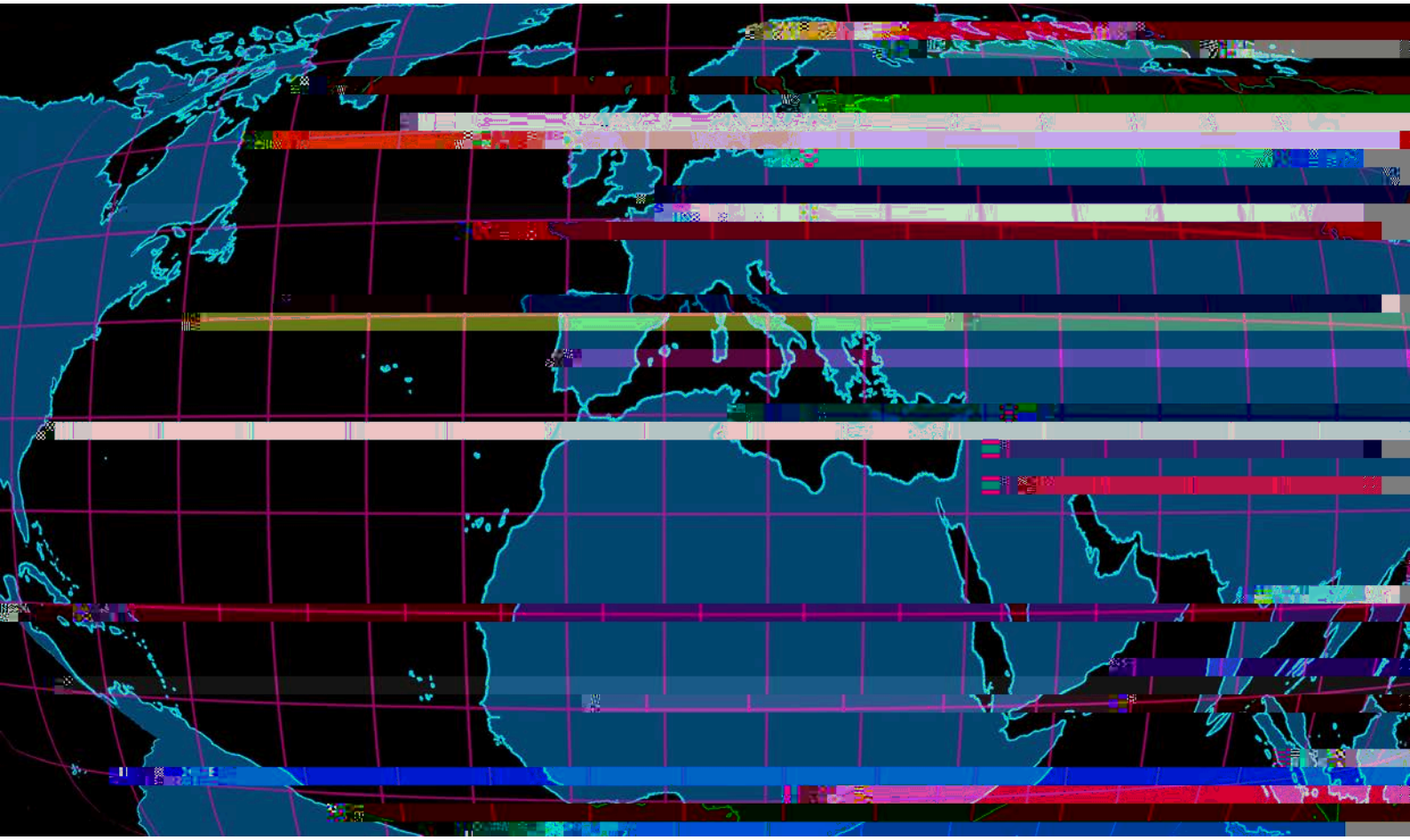
gsin
GLOBAL SECURITY AND INTELLIGENCE NOTES
March 2021
BUCSIS
Centre for Cybersecurity and
Intelligence Studies

Petros PETRIKKOS and Marinos PAPAIOAKEIM

Hybrid Threats in Small States: The Case of the Republic of Cyprus



THE UNIVERSITY OF BUCKINGHAM

backed approach to study the capacity of small states in withstanding modern threats, such as cyber threats.[6]

There have been several attempts to define small states and provide a widely acceptable definition, but mos ())Tj -0.00f8v9f 0y td pnihnmtmse1 (at)ec-3.452 -1.391 Td27.879 (he)nde-1 (ay)38 (t)sc.(o

This specific interpretation explains that hostile action can be initiated by state or non-state actors alike, often targeting states and institutions,

that are directly relevant to small states alone. Our analysis focuses, exactly, on this unique relationship between hybrid threats and small states. While it becomes apparent that a dominant security issue for small states often revolves around geographical size and population, nevertheless such states have the capacity to protect themselves by utilising the international system to address their security needs and defend their interests, not only militarily but mostly diplomatically, and to exercise adequate deterrence and pressure against their perceived adversary.[15]

Similarly, due to their own capacity limitations, in both quantitative and qualitative aspects, small states can be easily targeted by a hostile entity using, simultaneously, conventional and unconventional means. Warfare does not merely take place physically in the battlefield alone. In principle, vulnerabilities are exploited by understanding the opponent's capabilities.[16] The same can be said for using these capabilities in order to reduce the security gap created by such vulnerabilities. While war and conflict are means through which an actor accomplishes a political objective, it is a costly process. Selecting different alternatives to accompany or substitute armed hostilities and to deliberately spread insecurity against a targeted state or society, is often a more effective way of conducting operations with much less casualties and a limited cost.[17] Consequently, an aggressive adversary, using hybrid means and unconventional methods, may exploit infrastructural flaws, policy deficiencies or existing security gaps to implement significant political objectives without resorting openly to armed violence.

Therefore, small states with underdeveloped security infrastructures and limited or obsolete defence apparatuses are particularly exposed to these types of threats, notwithstanding any already-present conventional threats. Hostile entities pursuing this pathway may prevent effective decision-making, thus incapacitating both state and societal response to combat these threats. Not only that, but small states cannot appear weak within international institutions and blocs they hold membership to, as they might be seen as unreliable partners and threat-attracting liabilities. For this reason, they might opt to frame their own position and capabilities in such a way so that they retain a positive image of themselves. To do so, however, they also need to refine their security approach.

Security gap: vulnerable and unprotected

Vulnerabilities arise from a variety of reasons, including the absence of adaptability, in other words, failing to adjust to new threats. The problem with hybrid threats is that it is difficult to predict the best course of action towards an integrated security approach, particularly when there are weak or questionable institutional mechanisms in place. Furthermore, it is often diff-195 (of195 (w)1)-25 (i)-1 (t)-1 ( )-2

default, much slower in mobilising its security and defence services to combat the challenge.[18] Having said that, not only do states find it extremely difficult to identify and intercept hybrid threats, when an institutional framework is deficient, but this generates additional anxiety and insecurity across the social fabric.[19]

Capabilities: renewed means of deterrence

Despite these challenges, there are also merits and opportunities for small states to retain a degree of flexibility and adaptability when dealing with such threats. The real question is related to the attribution and tracking of the origin of such threats. In the case of the RoC, as is explored in the latter part of the essay, this is often easily identifiable, as most threats emanate from the Republic of Turkey. It is noteworthy to acknowledge the real and practical limitations of small states, especially their own position in the international system. This allows small states to revise existing institutional limitations by: (a) improving the infrastructure across varying state apparatuses, bringing them up to date with contemporary challenges; (b) educating civil servants and the wider society to be more alert against privacy and security issues, and to identify distorted and fake information; and (c) developing a unifying, common culture of security that can bring forth resilience, both at state as well as societal level.[20]

occupation of its northern part and a long-

Hybrid spillover effects of Turkish military provocations and violations against the RoC

The Turkish invasion of Cyprus in 1974, the consequent military occupation of 37% of the island's territory and the presence of approximately 35,000 heavily equipped Turkish troops in the occupied area, is a constant, existential, military threat for the RoC. As was noted by the Republic's minister of Defence, Charalambos Petrides, during an interview "Turkey is a constant threat for the security of Cyprus and has a large number of military presence in the occupied part of the island".[28]

Turkey and

leadership and the society, is an intentional tactic to achieve hybrid objectives through the use of military and political coercion, extending beyond state-to-state relations and impacting the social collective. Likewise, the intentional harassment of foreign vessels conducting seismic surveys or drilling operations on behalf of the Republic, such as the forceful obstruction, by Turkish naval vessels, of an Eni drilling ship in 2019, presents another example that encompass hybrid spillover effects. Since the RoC's image as a reliable partner in impin encompa2575Td [(th)1 (e)1 ( )-e

In December 2021, the Cypriot president characterised, during a summit in Brussels, the instrumentalization of immigrants from Turkey as “unacceptable”. The president also stressed the need for the EU to take effective measures to prevent such phenomena, both by Turkey and by any third country that exploit human suffering, in an effort to reap foreign political benefits. At the same time, he underlined that “the increased flows are mainly due to the instrumentalization of migrants from Turkey and their systematic and deliberate promotion through the green line [“buffer zone”], in the free areas [of the Republic], in violation of its obligations arising from the EU-Turkey Declaration of 2016”.[44]

Cyber Threats

Cyber threats are not easily detected in advance, until during or after the attack, and state-actors often suffer in the attribution of responsibility for threats in the cyber domain.[45] Furthermore, it becomes difficult to pre-emptively identify and take measures against such threats before they take place.[46] Cybersecurity specialists on the island have begun identifying various cases of cyber-attacks against local targets. Certain incidents denote that the RoC faced a cyber-attack connected to Turkish-sponsored stakeholders.[47] Such was the case when a cyber-attack attempt, aiming at data breach or damage in the Ministry of Defence website, took place in March 2021.

According to Ministry sources, the attack was successfully intercepted and no damage was caused to the operation of the website. As reported, Root Ayyildiz Turkish Defacer, branded as the “Father of Turk hackers” was planning on launching an attack against critical infrastructure in Cyprus, targeting mainly banking institutions and government services.[48] In another case, in January 2020, security experts cited by Reuters claimed that the Cypriot government internet traffic and emails have previously been attacked by Ankara-sanctioned hackers back in 2018 and 2019.[49] According to the report, hackers acting on behalf of the Turkish government were thought to be responsible for the sweeping cyber-attacks against governments, banks and other organisations in Europe and the Middle East.

Disinformation / Fake News

An indicative recent example of disinformation by Turkey was a coincidental event that took place in December 2021, when a 27-year-old Syrian refugee started a fire in an Islamic mosque in Larnaca

[44] “N. Anastasiadis: The instrumentalization of immigrants by Turkey is unacceptable”, News Bulletin, 16 December 2021, https://newsbulletin247.com/world/21832.html; “N. Anastasiadis: Cyprus faces hybrid threats from Turkey on the issue of immigration”, The President, 22 October 2021, https://www.thepresident.gr/2021/10/22/n-anastasiadis-i-kypros-antimetopi-me-yvridikes-apeiles-apo-tin-toyrkia-sto-zitima-toy-metanasteytikoy/.

[45] Joe Burton, “Small States and Cyber Security: The Case of New Zealand”, *Political Science*, 65:2 (2013), 216-238 (237).

[46] Aaron F. Brantly, “Entanglement in Cyberspace: Minding the Deterrence Gap”, *Democracy and Security,* 16:3 (2020), 210- 233 (211).

[47] Jack Stubbs, Christopher Bing, and Joseph Menn, “Exclusive: Hackers Acting in Turkey's Interests Believed to be Behind Recent Cyberattacks - Sources”, Reuters, 27 January 2020, https://www.reuters.com/article/us-cyber-attack-hijack-exclusive-idUSKBN1ZQ10X ; “Cyber-attacks on Turkey and Cyprus”, [illegible]

after the imam refused to let him sleep in the mosque for the night.[50] Considering that the perpetrators were Greek Cypriots – before the full disclosure of the details – the Turkish president Recep Tayyip Erdogan took advantage of the opportunity to warn that the incident "will not go unanswered" and the alleged Greek Cypriot perpetrators "will pay a heavy price".[51] Similarly, in January 2022, the Turkish Foreign minister Mevlüt Çavu!o"lu, speaking in Estonia, went as far as to claim that both the Hellenic Republic and the Republic of Cyprus – two EU member states – are terrorist hubs and will "pay the price", noting how the RoC, in particular, is allegedly a haven for Syrian Kurds that are associated with the Kurdistan Worker's Party (PKK) and the Syrian Kurdish People's Defence Units (YPG).[52] While this particular claim has not been supported by evidence, such statements are intended to excuse potential future aggressions in the area, in a narrative that conveniently fits the Turkish objectives against the RoC.

Notably, the "paying the price" narrative is exhibited in both incidents as a means of directly threatening the Republic. Disinformation against the RoC is targeted in two ways: (a) it allows Turkey to use the Republic of Cyprus as a scapegoat in the international political arena for various incidents, and

often been slow in its responses or utterly oblivious when it comes to similar crises experienced in

framework for the formation of Computer Security Incident Response Teams (CSIRTs).[60] Until late 2021, however, the CSIRT project was dormant and only one CSIRT was, in fact, active.[61] At the time of writing, there are two fully accredited teams that are part of the CSIRT network as listed on the ENISA website, whereas the Republic of Turkey has a total of seven such teams.[62] While Cyprus managing two teams is incomparable to how the larger Turkish resources allow for seven such teams to be managed, size in this case does not matter. CSIRTs are ideal tools to mitigate and prevent cyber disasters within states and societies.[63] They are also responsible for filtering disinformation and fake news. Without strong infrastructural guidelines on this, states and societies become susceptible to distorted realities. By leaving key infrastructural communication systems underdeveloped, the state unnecessarily exposes itself to additional security risks.

Furthermore, addressing the problem of underdeveloped infrastructure, the economic and

cybersecurity practices. In terms of policing, the Republic has working frameworks that focus on a combination of civilian and intelligence security practices. The Cypriot intelligence agency KYP (whose initials translate as “Cypriot Information Service”) is an example of such a service that was left unregulated for decades (1970-2016),[68] with no legal framework in place to check on its unseen powers. Following a scandal in 2015, which revealed that KYP was spying on phone communications,[69] the unchecked powers of the intelligence agency were immediately recognised as a serious vulnerability, prompting lawmakers to urgently address it through regulation.

Similarly, the state needs to invest more on securing governmental online spaces. While there is a great level of investment in corporate cybersecurity training, only small steps are undertaken in translating this to policy needs. Characteristically, cybersecurity training programs, often, rely on the technical and not so much on the implementation phase across institutions. Real expertise is lacking, yet this is hopefully going to be addressed with the introduction of a proposed Digital Academy in 2022, as it was reported by governmental stakeholders in the media.[70]

RoC Capabilities

While it is ultimately easy to paint an overall negative picture to depict these hybrid security challenges, it must be emphasised that there are noteworthy attempts in the making for addressing these

5271hd.-7812h2c(r((2)32)-.fs6o2-0-12382Dac26405)

e02o4o404
-.p031.-n54022.0-psd3173-s.37eSe..291(een1)

College (ESDC), it has hosted seminars on cybersecurity practices across the wider regional cyber ecosystem.[72] Another example, is the joint naval-air activities and exercises with other states, such as France, Israel, Egypt, Greece, the United Kingdom and the United States, that have increased in the last decade, providing maritime awareness in the Eastern Mediterranean.[73] Such activities enhance the image of the RoC as a reliable security and defence player. Moreover, joint exercises can be used as an important diplomatic tool, as an expression of mutual trust and friendship while reassuring allies of the Republic's intentions. These defence diplomacy activities assist the development of a positive geopolitical image for the RoC.

Such collaborations have been possible due to the Republic's membership in international institutions such as the European Union and in its security and defence frameworks like the Common Defence and Security Policy (CSDP), the European Defence Agency (EDA) and the Permanent Structured Cooperation (PESCO). Moreover, it plays an important role in cultivating educational awareness, training and establishing a common strategic and security culture.[74] The question of leadership, institutional cultural and the availability of suitable tools in implementing security policies are crucial within any institutional environment, especially for a small state like Cyprus.[75]

Conclusion - Reflections

Small states and societies exper al es s ovietionas s naliesSmy2 (e)-1 (s)-1o ( )-f1 (n)t1 (o)-1 (v)n1 (i)-1 (s)-1