Small yet Smart:
How Emerging Technology Enables Small Powers to Survive

Axel D'Amelio
A Thesis
in
International Relations

Presented to the Faculties of the University of Pennsylvania in
Partial Fulfillment of the Requirements for the
Degree of Bachelor of Arts

April 2025

_____
Farah N. Jan, PhD.

Acknowledgements

To my many mentors– Dr. Casey Mahoney, Dr. Frank Hoffman, Nadia Schadlow, and Michael Dressler– for all taking me under your wings and trusting me with your work and allowing me to grow. You have all ignited my curiosity, and your mentorship has been invaluable. Thank you all for giving me a chance.

To Dr. Mitchell Orenstein– for being my guide during my time at Penn. From adding me to the database team to introducing me to FPRI to leading me on an adventure throughout Europe.

To Mom, Dad, and Chloe– for the unrelenting love, support, and belief you have provided Penn. You were all there for any of my problems, concerns, or stresses. I do not know what I would have done without you all.

To Amelia, for listening to my complaining and stress, which you endured patiently. You were always there to offer a listening ear and stood by my side as I worked into the dark hours of the night.

To Dr. Jan, for being an incredible professor, advisor, and mentor. I will forever be grateful for our first introduction in INTR 2900. The passion you dedicate to your craft and your students is inspiring. Thank you for believing in me despite my terrible communication skills and inability to meet deadlines. I will forever be indebted to your guidance.

Thank you.

Abstract

The following thesis asks the question: How does emerging and disruptive technology (EDT) impact the resilience of small powers? Small powers have regularly been discounted from debates on power and influence due to the fact that they are limited by size, population, resources, and strategic depth. With that said, this thesis challenges this notion by presenting a certain type of small power through the *Small, Smart Power Model*. This research suggests that there exists a certain group of small powers that have embraced their smallness and transformed their structural vulnerabilities into strength by becoming smart. Smallness and smartness serve as mechanisms for survival as these small powers innovate EDTs, restructure at the operational level, and implement asymmetric strategies. Conducting comparative case studies on Ukraine, Estonia, and Singapore, this thesis finds that a total defense approach is key to the success of this club of small, smart powers. Uniting the entirety of their populations behind the mission of defending the nation, these states use technology as a lifeline for their entire societies to contribute. Through this whole-of-society approach based on mobilizing EDT innovation, these states enhance resilience. Thus, this thesis finds that resilience is not simply the ability for these powers to recover from threats but is a deterrent force that can be signaled to potential adversaries. In sum, the findings of this research aim to contribute to the scholarly discussion on small powers, security, and technology by presenting a new theoretical model to conceptualize how weakness can produce strategic innovation.

Table of Contents

Chapter I: Introduction

If you think you are too small to make a difference,
try sleeping in a closed room with a mosquito.
– West African proverb[1]

The terms small state and military power have rarely been used together. Small powers are often perceived as limited in their capacity to respond effectively to larger and more powerful adversaries. They may possess neither the same manpower nor the level of resources to stand against a great power, let alone inflict meaningful costs. Yet, as global security dynamics evolve, such assumptions warrant closer examination. Lithuania exemplifies the dilemma: although its population of just 2.8 million and a GDP of $77.84 billion might seem uninteresting, its strategic position in the Suwalki Corridor—separating Belarus from Russia's Baltic enclave of Kaliningrad—places it on the eastern frontier of the North Atlantic Treaty Organization (NATO).

From the Russian perspective, Lithuania presents a problem. It blocks Vladimir Putin from having full Baltic Sea access, which would provide direct access to the Atlantic Ocean. Additionally, Lithuania is the direct manifestation of one of Putin's strongest grievances that the West is encroaching on Russia's borders and does not respect his say. Lithuania's NATO and European Union (EU) membership and growing military capabilities, particularly in cyber defense, represent what Putin views as Western technological encirclement. Lithuania also serves as an example of a former Soviet state that has joined Western institutions and modernized its military. This threatens Putin's narrative about the necessity for Russia to preserve its sphere of influence. Moreover, Lithuania's vocal criticism of Russian aggression and its strategic support for Ukraine demonstrate how small powers can resist Russian power.

[1] Godfrey Baldacchino, "Thucydides or Kissinger? A Critical Review of Smaller State Diplomacy," *The Diplomacies of Small States*, 2009, 21–40, https://doi.org/10.1057/9780230246911_2, 26.

From the Lithuanian perspective, Russia's history of aggression poses an existential threat. The Kremlin's behavior with the invasion of Georgia in 2008, annexation of Crimea in 2014, and the full-scale invasion of Ukraine in 2022 suggests that the invasion of a NATO frontier state may not be out of the realm of possibility. This increased pattern of aggression is combined with the increasing hybrid war that Russia has waged against Western and Central Europe. Lithuania has taken measures to increase its security by joining NATO, but its security is not ensured. Additionally, the uncertainty attributed to Donald Trump's second presidential term and his threat to leave NATO poses a risk to European security as a whole, let alone Lithuania. Without its primary security guarantor in the United States and the dismal state of European Union military forces, Lithuania must find solutions to guarantee its own security if the hypothetical conditions previously mentioned come true.

The Fourth Industrial Revolution has arrived and presented Lithuania with a potential solution to its inherent smallness. Characterized by systems of systems, emerging and disruptive technology (EDT) has risen, transforming conventional war. Today, drones swarm the skies operated by artificial intelligence, destroying tanks and planes. Conventional war is changing before our eyes, and the character of warfare is transforming with it. The future of warfare is becoming faster and cheaper, yet not all states are adapting to this reality. Additionally, war and conflict are increasingly creeping into non-kinetic realms through the use of hybrid war tactics. EDT presents states with a new, affordable option to fight back. Many small powers have an option to bolster their security by developing grassroots technology that does not rely on the heavy resources and capital that conventional systems developed by greater powers do. Therefore, this paper asks the following question: How does emerging and disruptive technology (EDT) impact the resilience of small powers?

The paper predicts that by harnessing and strategically deploying this new wave of technology, small powers can better defend themselves and become more resilient. The hypothesis is based on the logic that EDT allows smaller powers that might classically be constrained to spending their defense budgets on a limited number of expensive legacy arms and technology to use innovative, flexible strategies to maximize their defensive capabilities and strategic impact while optimizing costs. In the non-kinetic realm, EDT also allows small powers to develop responsive measures to defend against rising hybrid threats. Thus, small powers can develop unconventional, irregular technology and asymmetric strategies to become more resilient against great powers.

In the following sections, the thesis will explore the terms small power and great power. It will look into the discussion of how small powers fight, specifically when facing a great power. It will also define the terms EDT as well as resilience. Moving from this literature review and definition of terms, it will introduce its theoretical framework and research design. It will introduce the *Small, Smart Power Model,* which proposes a new model or type of small power. From this model, the paper will investigate how EDT has enabled small, smart states to increase their resilience against threatening powers. The paper will delve into three case studies looking at Ukraine, Estonia, and Singapore.

This paper primarily aims to add to the discussion on small powers in several ways. The international system is entering a period of great uncertainty. Great powers are no longer the sole centers of progress and innovation as the power of technology has diffused across the globe. This paper aims to present an account of how small powers can increasingly compete in this new system. While smallness has traditionally been regarded as weakness, this paper aims to reveal its potential for strength. Small powers have a distinct survival instinct that has forced them to learn

and adapt rapidly. Thus, the paper also aims to present this agile, innovative trait of small powers as one that all powers ought to learn from as well. Small powers can provide an alternative account for all powers on how to survive and prosper in an uncertain, dangerous world.

Chapter II: Literature Review

The guerrilla wins if he does not lose.
The conventional army loses if it does not win.
– Henry Kissinger[2]

To truly understand the role emerging technology plays in small powers' asymmetrical approach to defending themselves against great powers, this thesis will define these three terms. The first section aims to define what is meant by a *small power* as well as elucidate the shift in discourse on small powers. It will also look at the discussion of why certain small powers have been able to successfully fight back against great powers. It will focus on small powers' asymmetrical or unconventional strategy as the key to this success. Next, it will define technology through the concept of emerging and disruptive technology. Finally, it defines resilience to shape the last piece of the puzzle that this thesis aims to solve.

The International System and the Security Dilemma

This thesis assumes the international arena to be an anarchic system where each country must do what it can to ensure its own survival. Under this realist framework, no singular power or actor exists that oversees all other states and forces them to fulfill promises or prevent them from using violence to attain their goals. Defensive realists believe that the world is a self-help arena. In order to survive, states seek security to compete and balance against potential threats. According to Kenneth Waltz, the world forms a balance of power system where states focus on self-preservation instead of direct aggression.[3] Offensive realism, on the other hand, posits that states covet power and enact power-maximizing measures to pursue their aims.[4] John Mearsheimer argues that states

[2] Henry A. Kissinger, "The Vietnam Negotiations," *Survival* 11, no. 2 (February 1969): 38–50, https://doi.org/10.1080/00396336908440951, 39.
[3] Kenneth Waltz, *Theory of International Politics*, 1st ed. (New York: Random House, 1979), 199.
[4] John Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Company, 2014), 43.

have an insatiable desire for power with the ultimate aim of becoming the singular hegemon. Due to the fact that it is unlikely for a single state to become the global hegemon, Mearsheimer claims that the world will become a competition between great powers going to war with each other.[5] Thus, offensive realists view states as power maximizers while defensive realists take states to be security maximizers.

Both schools of realism base their logic on the security dilemma. Greatly shaped by Robert Jervis, the security dilemma presents a model that explains how states make decisions within the international system.[6] For Jervis, states have two options: cooperate or defect. The best option for all states is to cooperate and disarm. States, however, are uncertain about one another and cannot fully know and view the price of one state defecting to be too costly. Thus, states maximize their security by whatever means possible, whether it is defensive or offensive capabilities. The security dilemma arises when states increasingly build their military capabilities and eventually spiral into war. Under the spiral model, states may choose to go to war either out of preventive or preemptive measures. Jervis outlines the different outcomes when offense or defense is favored. When offensive and defensive measures taken by states are indistinguishable, but offense has the advantage, states will act aggressively, and an arms race is likely. When offensive and defensive measures taken by states are indistinguishable, but defense has the advantage, states will act to increase their security but not in a threatening way to other actors. When offensive and defensive measures taken by states are distinguishable, but the offense has the advantage, the environment is safe, but the future conflict is still possible. When offensive and defensive measures taken by

[5] Ibid, 44.
[6] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214, https://doi.org/10.2307/2009958.

states are distinguishable, but defense has the advantage, the danger of aggressive behavior is low, and states feel safe.

What is a small power?

The attempts to define small states have largely depended on realist assumptions of the international system and state actors. Geography, resource base, territory, and population are all commonly measured to determine power. Certain states hold greater access or higher levels of these determinants of power and are therefore considered to be more *powerful*. Under this logic, the terms *small state* and *military power* are rarely used in the same sentence. Given the assumptions of the realist model, small powers have largely been considered irrelevant. According to offensive realism, the claim that great powers run the international arena would suggest that there is a certain point it becomes pointless for small powers to invest in military capabilities since their militaries could never stand a chance against those of great powers. Building a military might seem like a waste of time and money for small powers, yet they still develop their own military capabilities.

The scholarly literature on small powers has long focused on their struggle for survival, leading to a gap in discourse on small powers deciding to seek military power and wars of their choosing.[7] As the international system has developed, however, this narrative that small powers struggle to survive or hold little influence has been proven wrong. To quote Robert Keohane, "[if] Lilliputians can tie up Gulliver, or make him do their fighting for them, they must be studied as carefully as the giant."[8] Small powers are not defenseless. History has shown cases where they

[7] Manish Jung Pulami, "Analysing Revitalised Security Industry: The Tech-Powered Transformation for Small States," *Unity Journal* 5, no. 1 (March 25, 2024): 301–15, https://doi.org/10.3126/unityj.v5i1.63195, 303.
[8]Robert O. Keohane, "Lilliputians' Dilemmas: Small States in International Politics," *International Organization* 23, no. 2 (1969): 291–310, https://www.jstor.org/stable/2706027, 310

successfully defend themselves and even defeat greater powers. The reasons for why, however, are understudied. Thus, small powers require greater focus.

To begin, a definition of great powers is necessary. As defined by Jack Levy, great powers are states that hold a major role in the international system and maintain global security interests.[9] Great powers oversee military control within their borders and project military power both within their region and beyond. They do so independently, actively protecting their interests, forming alliance networks, and engaging in wars. A key sign of a great power is that their status is recognized by other states, which further validates their positions in international organizations, diplomatic relations, and treaties.

The literature covering the concept of small powers and international relations has seen a variety of debates over the past four decades. The disagreements over how to define the term *small power* have been so strong that some have claimed there is "no internationally established or academically agreed upon definition of the 'small state.'"[10] The original distinction between small and great power originates from the beginning of the 19th century during the Napoleonic Wars. Great powers viewed small powers as states that were too weak to defend peace agreements and the international order to create peace. This view evolved over the course of the 19th and 20th centuries and experienced a substantial shift with the creation of the League of Nations. The League of Nations created a setting where small states could be heard and exercise significant influence. During the interwar era following WWI, the discussion of small states focused on their growing position within international organizations. The end of World War II marked another big shift as countries decolonized and empires collapsed. Most notably, Annette Baker Fox's work,

[9] Jack S Levy, *War in the Modern Great Power System: 1495-1975* (University Press of Kentucky, 1983), https://doi.org/10.2307/j.ctt130jjmm.
[10] Alan K. Henrikson, "A Coming 'Magnesian' Age? Small States, the Global System, and the International Community," *Geopolitics* 6, no. 3 (December 2001): 49–86, https://doi.org/10.1080/14650040108407729. 56.

The Power of Small States, from 1959 marked a new wave of scholars who focused on small state survival tactics and alignment strategies during great power conflicts. During the Cold War, small powers were studied in relation to how they could survive within the great power competition and contribute to the international system despite their limited power and capability. The 1970s focused on dependency and economic cooperation as the international relations field focused on topics related to political economy, interdependence, and international organizations. The 1970s marked a peak in the study of great powers due to a wave of decolonization. The 1980s and 1990s saw a standstill in the study of small states due to greater focus on great power competition.[11] Following the end of the Cold War, however, the study of small powers saw a strong revival as globalization and regional integration reignited new debates about small states' economies and foreign policies. The birth of new states as well as the creation of multilateral and international organizations sparked a renewed interest in the strategies of small states.

Despite the extended history of small power studies, there is still little consensus on the definition of a small power. David Vital proposes an absolute definition for small powers, setting the bounds at having less than 10-15 million inhabitants for advanced countries or less than 20-30 million inhabitants for underdeveloped countries.[12] The problem with the absolute definition of small powers like Vital's is that they are time-bound and treat the relationship between population, geography, and power as unequivocal. Just because a state might have fit within the population bounds 100 years ago, like the United States, this does not mean they are currently a small power. The same goes for states that may have been great powers, like the Netherlands, which oversaw tens of millions of people, including its territorial holdings during the early 20th century, but are

[11] Christine Ingebritsen et al., *Small States in International Relations*, *JSTOR* (University of Washington Press, 2006), https://www.jstor.org/stable/j.ctvcwnw88, 10.
[12] David Vital, *The Inequality of States* (Oxford: Clarendon Press, 1967), 8.

now considered small powers. Robert Rothstein defines a small state as a state that relies on the help of other states because it cannot guarantee its own security by itself.[13] He outlines three specific determinants of a small state: it depends on outside aid for its security, it has a limited space of maneuver and little room for correcting potential mistakes, and its political leadership sees its weakness as unalterable despite their actions. Keohane considers a state to be small if its leaders realize that, in acting alone, they will fail to impose a significant impact on the system.[14] Here, the distinction between the absolute and relational definition of small states arises. If the definition of a small power is not absolute, then how can the framework adequately address the disparity in states ranging from microstates such as Lichtenstein to countries which have immense populations yet are still considered small like Indonesia?

Instead of trying to find a universal definition of a small state, scholars have proposed that the concept of small power should be used as a focusing device instead of a strict analytical tool. Thus, the concept of a small power highlights the security problems and foreign policy concerns of weaker powers in asymmetric relationships. That is why this thesis uses the term small power instead of small state to highlight that smallness depends on a power dynamics. Smallness is taken to be a measure of power not against all other states or a singular source but studied in relation to the neighbors of the small power and according to the degree to which the strength at its disposal matches its national goals and ambitions.[15] This allows for a small power to be small in certain relational power configurations and great in others. This thesis follows Adam Raska's definition of five characteristics which form the base of "smallness": relative asymmetries of the location, geography, and size; demographic, economic, and natural resource constraints; dependence on

[13] Robert L Rothstein, *Alliances and Small Powers* (New York: Columbia University Press, 1968).
[14] Keohane, "Lilliputians' Dilemmas", 295-296.
[15] Michael Raska, *Military Innovation in Small States* (Routledge, 2015), 11.

external political and material support; security uncertainties or proximity to areas of conflict; relations and importance between and to great powers.[16] These factors shape the common feeling of insecurity and desire to survive that determines small powers' approach to security. It is also important to note that a defining characteristic of small powers is that they desire peace. Small powers understand that they are at a disadvantage in the international arena, especially when acting alone. Thus, they desire peace as the status quo within which they can operate. Traditionally, this manifests itself in small powers being staunch supporters of international organizations because they allow the small to voice their interests. That said, international organizations and cooperation are not the sole means to achieving peace. Returning back to the realist view, defense, security, and specifically deterrence can serve as a solution to producing peace.

Irregular, Asymmetric, and Unconventional Strategies

Moving from the definitions of small and great powers, the question why small powers have militaries returns. The realist view takes military capability to define power and a higher concentration of power to imply victory in war. Based on this view, greater powers should always win against a weaker power. It would seem pointless for a small power to build up national military forces and suggests pursuing peaceful diplomatic strategies to avoid war and ensure survival to be more logical. History, however, disproves the assumption that great powers always defeat small powers. Instead, small powers do win sometimes. Beyond winning against great powers, some small powers go so far to initiate wars against great powers.[17] Over the course of history, great powers have fought small powers surprisingly poorly. It is not so much that the great powers lose

[16] Ibid, 12.
[17] T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers*, vol. 33 (Cambridge University Press, 1994).

to small powers, but more so that great powers fail to win.[18] The question then rises: how do small powers win?

Some realists have attempted to explain why small powers win; however, they attribute the victory to the greater powers and not the smaller power. Specifically, Robert Gilpin and Jeffery Record present two separate explanations. Gilpin argues that a hegemonic power experiences decreasing marginal returns after reaching its historical peak. As the empire expands, the cost of maintaining the empire increases, and the empire goes into decline.[19] Within the empire's territory, an increase in resistance and challenge to the great power grows proportionally as the great powers decline. Gilpin attributes the ability of weaker powers to defeat greater powers to the greater power's loss of control and gradual decline. Jeffery Record presents an alternative explanation, which has been named the theory of foreign assistance. Record argues that, in almost all cases of asymmetric conflict where the weak power defeats the strong, the weak power received foreign assistance that reduced the gap in military advantage between the two actors.[20] While both arguments maintain some validity, they underestimate the agency and power of the smaller actor in asymmetric conflict.

In response to the material power explanation, some scholars explore the concept of asymmetry and asymmetrical motivation. In "Why Big Nations Lose Small Wars," Andrew Mack argues that the relative resolve of an actor provides an explanation for their success in asymmetric conflicts.[21] Mack's argument is better known as the interest asymmetry argument. Because weak powers fight for their survival when faced with a greater power, they are prepared to absorb the

[18] Robert M. Cassidy, "Why Great Powers Fight Small Wars Badly," *Military Review* 82, no. 5 (September 2002): 41–53, https://apps.dtic.mil/sti/pdfs/ADA489552.pdf, 1.
[19] Robert Gilpin, *War and Change in World Politics*, 1994, p. 228.
[20] Jeffrey Record, 'Why the Strong Lose?' Parameters, Vol. 35 (2005/06), pp. 16–31.
[21] Andrew J.R. Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict," *World Politics*, Vol. 27, No. 2 (January 1975), pp. 175-200.

costs of long wars. In these cases, greater powers have low interests yet take on high costs. The weak power wears down the political will of their opponent until the ruling elite of the greater power faces political vulnerability from domestic pressure and therefore pushes to end the war before victory.

In response to Mack, Ivan Arreguin-Toft argues that strategic resolve best predicts the outcomes of asymmetric conflict, also known as the strategic interaction hypothesis. In "How the Weak Win War," Arreguin-Toft investigates the different approaches between small and great powers during military confrontation. He outlines two options which both the stronger and weaker powers have in conflict: direct or indirect approach. In both approaches, the strategies of actors may be offensive or defensive. Arreguin-Toft finds that same-approach interactions, that when the strong and weaker power both take a direct approach or both take an indirect approach, favor the stronger power.[22] This is because the stronger power has stronger raw power and goals in these scenarios that prevent other factors from intervening. Opposite-approach interactions, on the other hand, favor the weak actor because the smaller actor refuses to engage where the greater power has a power advantage.[23] The smaller power often prolongs conflicts and delays the objectives of the greater power.[24] In this delay, the public or opposing elite have time to question the goals, morality, costs of the conflict and deem it illegitimate. At this point, the stronger power becomes politically vulnerable as the political elite must choose to end the conflict prior to victory, bending to domestic pressure, or continue an unpopular war, inflaming political tensions. An objection to Arreguin Toft's argument is that time works to the disadvantage of the weak. While many cases where the weak prevailed over the strong include prolonged wars where time was important, there

[22] Ivan Arreguin-Toft, *How the Weak Win Wars A Theory of Asymmetric Conflict,* PAGE 121
[23] Ibid, 105.
[24] Ibid, 122.

are also many cases where the strong power wins prolonged wars. Therefore, the concept of cost in relation to time must be considered.

The consideration of time alongside cost leads to a discussion of what indirect strategies manage to combine these two aspects. Sandor Fabian presents four main military strategy options for small powers to pick from: imitating the conventional military approach of a great power, joining an alliance, claiming neutrality, or acquiring weapons of mass destruction.[25] Each of the options has high risks though.

Given the vast difference in physical capability and spending power between a small and great power, it is very difficult for a small power to imitate a great power. As a result, a small power might seek an ally; however, this is risky as well since the small power's security depends on the stronger partner honoring its promise. This might leave the small power entirely alone. Within an alliance, the small power faces a separate problem of how to shape its forces. Does it mirror the approach of the stronger allies replicating their conventional approach or focus on a few specific tasks to make up a combined allied force? In either case, if the alliance fails, the small power is left with a weak conventional force or highly specialized force with gapping vulnerabilities. The alternative option of assuming neutrality depends entirely on other states respecting the terms of neutrality and understanding the potential costs of invading a neutral country. Finally, pursuing weapons of mass destruction is typically unavailable to most small powers. Therefore, it seems that the small power is left with no viable strategy.

Regardless of whether small powers pursue alliances or not, they must be willing to to an irregular, unconventional approach to defense and security. While not all or even most conflicts follow the same pattern, an asymmetric strategy offers a way for smaller powers to surprise greater

[25] Sandor Fabian, "Professional Irregular Defense Forces: The Other Side of COIN" (2021), https://apps.dtic.mil/sti/citations/ADA562847, 18–26.

powers and find ways to poke holes in their adversary's defense. Additionally, the reputation of having an unconventional strategy may even serve as a deterrent force against a greater power that is unwilling to risk defeat because it is unable to predict what opposing strategy the invading power will face. This leads to a discussion of how war and conflict are changing and therefore, how small powers can respond, learn, and apply new strategies. With the rise of new technology and tactics available with the rise of hybrid war, small powers have a wider range of possible indirect ways to deter and resist great powers.

What is Emerging and Disruptive Technology?

In some academic writing, the term emerging and disruptive technology is not defined but simply presented as a list of new technologies that are labeled as EDT. Additionally, the terms emerging and disruptive are often used interchangeably. This fluid use of the terms causes them to lose their unique defining force. Thus, it is important to review the varying definitions of the two terms that exist in the current literature. This section will properly define the emerging and disruptive individually as a foundation for the full, combined definition of emerging and disruptive technology.

According to NATO, the difference between emerging technology and disruptive technology is timescale. In its *Science & Technology Trends 2020-2040*, NATO defines emerging technology as technologies that need longer time horizons to mature and have a less determined development trajectory.[26] Daniele Rotolo, Diana Hicks, and Ben Martin give emerging technology five specific attributes: (i) radical novelty, (ii) relatively fast growth, (iii) coherence, (iv) prominent

[26] Neven Vincic, "The Future of Warfare: Security Implications of Emerging and Disruptive Technologies (EDTs)," NATO Association of Canada, May 12, 2021, https://natoassociation.ca/the-future-of-warfare-security-implications-of-emerging-and-disruptive-technologies-edts/.

impact, and (v) uncertainty and ambiguity.[27] Disruptive technology exists in a more advanced state of maturation. It is expected to or already has had a significant or revolutionary impact on the character of war and collective security and defense within 5 to 10 years.[28] Additionally, the technology can originate from non-traditional defense actors or be inspired from the civil domain.

Some scholars have introduced convergence as a third category which reconciles the concepts of emerging and disruptive technology.[29] Converging technology merges emerging technology with pre-existing, validated technologies *"in order to create new and better possibilities and allows development and maturation."* [30] The tank demonstrates the concepts of emerging, convergent, and disruptive technology. The tank first emerged at the beginning of the 20th Century, then gained popularity converging with previous technology like armor and radio during the interwar years and finally becoming disruptive during the blitzkrieg tactics of the German army.

Combing the terms together, this thesis takes emerging and disruptive technologies (EDTs) to be either technologies that are new and rapidly evolving but not yet proven, emerging, or technologies that have matured and been applied, reshaping current strategies, disruptive. This thesis follows the NATO STO's list of ten critical EDTS: Artificial Intelligence (AI), Robotics and Autonomous systems, big data (BDA), electronics and electromagnetics, hyper sonics, energy and propulsion, space technologies, quantum technologies, biotechnologies, and novel materials and manufacturing (NMM).[31] As these emerging and disruptive technologies become increasingly

[27] Daniele Rotolo, Diana Hicks, and Ben R. Martin, "What Is an Emerging Technology?," *Research Policy* 44, no. 10 (December 2015), https://doi.org/10.1016/j.respol.2015.06.006, 1
[28] Vincic, "The Future of Warfare".
[29] Harald Erik Andås, "Emerging technology trends for defence and security," Norwegian Defense Research Establishment, (2020).
[30] Andås, "Emerging technology trends for defence and security," 9.
[31] NATO Science & Technology Organization, "Science & Technology Trends 2023-2043," March 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

available and affordable, small powers have new means to create asymmetric strategies and enhance their resilience and do deter enemies. This, however, leads to the question: what is resilience?

What is resilience?

While resilience has been used as a term in a wide variety of fields like psychology, economy, and industry, in international relations it has been defined according to different terms by various institutions, most notable of all being NATO. This section aims to cover some of the different definitions of resilience and provide a foundation for agreement across the varying definitions. At its most basic level, resilience represents the ability to recover and adapt in response to adversity.

Resilience and resistance are two very different concepts. Resistance is the mobilization of a system's full set of resources to deal with the immediate effects of a stressor. The concept is based on a return to the status quo of the pre-stressor environment. Resistance is a deficient concept because it creates a persistent dysfunction in a system that rarely returns to pre-event circumstances.[32] In reality, a system shifts into an altered environment. Resilience, however, is the successful adaptation of a system to an event and the following recovery to a new set of conditions. Resilience is not just the ability to withstand stress but the "ability to find unknown inner strengths and resources in order to cope effectively with long-term pressures."[33] Thus, resilience is a measure of adaptation and flexibility.

[32] Tomas Jermalavičius and Merle Parmak, "Towards a Resilient Society, or Why Estonia Does Not Need 'Psychological Defence'," *International Centre for Defence Studies*, September 2012, 1–19, https://eprints.hud.ac.uk/id/eprint/21718/1/ParmakTowards.pdf, 5.
[33] Michael Ganor and Yuli Ben-Lavy, "Community Resilience: Lessons Derived from Gilo under Fire," *Journal of Jewish Communal Service* 79, no. 2/3 (2003): 105–8, https://coilink.org/20.500.12592/383f6s. 106.

Resilience encompasses three key dimensions. First, resilience involves deterrence through demonstrating that attacks will face unacceptable costs. For small powers, this means signaling that aggression will be met with protracted resistance and asymmetric responses. As NATO emphasizes, resilience stems from combining civil preparedness with military capacity to create layered defense. Second, resilience requires adaptive capability - the ability to adjust to changing circumstances and threats. This aligns a definition of resilience as adaptive, allowing structural factors to be resisted and reshaped. Small powers must be able to innovate and transform limitations into advantages through the power of powerlessness. Third, resilience demands both military and civilian integration. As highlighted in recent NATO doctrine, resilience requires whole-of-society approaches combining military defense, civil preparedness, and emergency planning. The Baltic states exemplify this by incorporating comprehensive resistance strategies into their national defense plans.

These elements together create an individual and collective capacity to withstand, fight through, and quickly recover from disruption. This modern conception of resilience particularly suits small powers facing hybrid threats, as it emphasizes adaptability and whole-of-society responses rather than just military strength.

What are the gaps in the literature?

While the previous scholarship has discussed the definitions, strategies, and vulnerabilities of small powers, this debate has often stopped at how small powers transform their inherent, structural disadvantages into strategic opportunities for increased security and influence. This thesis will reframe small powers not as passive actors but innovative, adaptive, daring powers able to leverage new technology to increase their resilience and deterrence capabilities. This thesis fills

a gap by developing the concept of resilience as deterrence, instead of presenting them as exclusive concepts. By connecting the concepts of EDT, unconventional defense, and resilience, this thesis addresses a critical gap. It aims to show how small powers survive and stand up to great powers, not by copying them but by outsmarting them.

Chapter III: Research Design

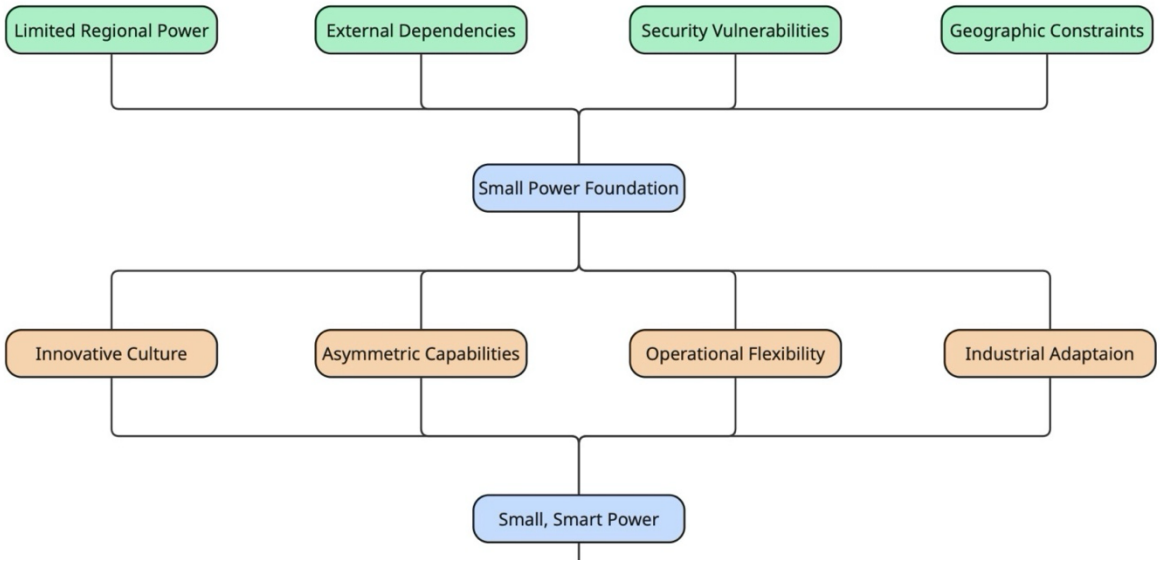
Introduction

This thesis aims to examine how small, smart powers can develop, acquire and implement EDT to act as survival artists and increase their resilience. It introduces the *small, smart power model* as a framework to understand how small powers use EDT to become more resilient. The following chapter outlines research design, methodology, and data employed in the study. By looking at the cases of Ukraine, Estonia, and Singapore, the thesis aims to support its hypothesis that EDT integration increases the resilience of small powers.

Theory & Variables

The essence of this paper's argument is twofold. First, this paper aims to argue that there exists a specific group of small powers which this paper calls *small, smart powers*. This argument rests on a foundational definition of small power based on the one given in the literature review. What makes this class of states small, smart powers is their understanding of their own smallness and embrace of this condition. What these small powers "lack in structural clout they can make up through creative agency."[34] These states harness the strength of powerlessness to become more agile and innovative in order to fulfill their intended policy outcomes. Thus, necessity gives birth to innovation. From this definition, the thesis suggests that there are certain conditions that define certain small powers as *small and smart*. The model can be seen below:

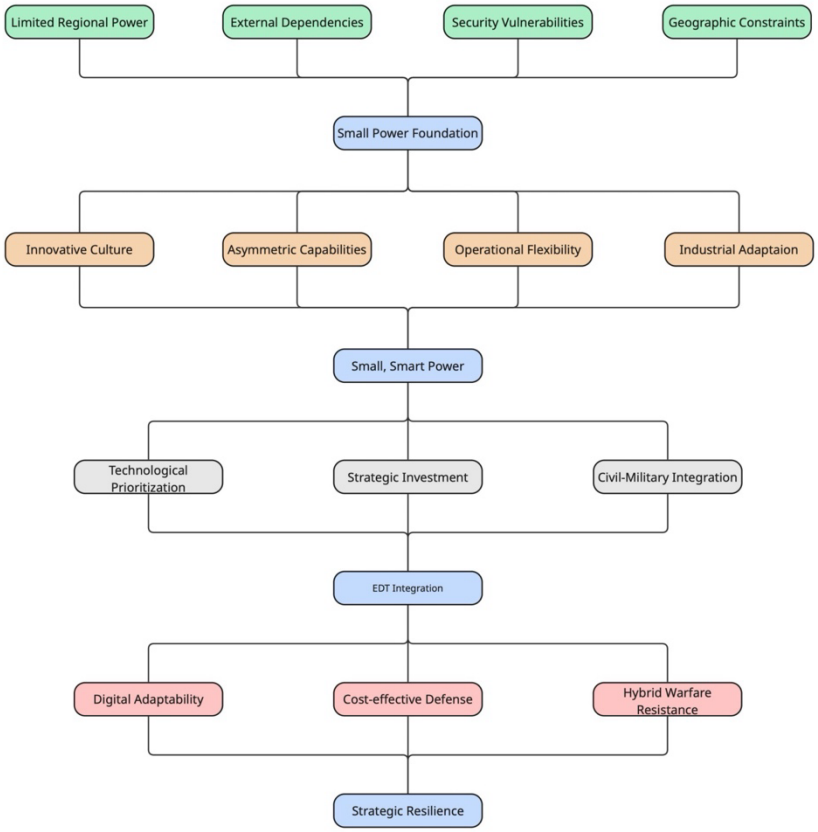
[34] Andrew I Cooper and Timothy M Shaw, "The Diplomacies of Small States at the Start of the Twenty-First Century: How Vulnerable? How Resilient?," in *the Diplomacies of Small States. International Political Economy Series* (London: Palgrave Macmillan, 2009), https://doi.org/10.1057/9780230246911_1, 2.



The second part of this paper's argument claims that small, smart powers are positioned to take advantage of and lead in certain aspects of the rising wave of EDT. It is here where "EDT," the independent variable of this study, comes into play. This paper defines EDT as either emerging technologies that are new and rapidly evolving but not yet proven or disruptive technologies that have matured and been applied, reshaping current strategies. To ground the definition of EDT, the thesis follows the NATO STO's list of ten critical technologies: Artificial Intelligence (AI), Robotics and Autonomous systems, big data (BDA), electronics and electromagnetics, hyper sonics, energy and propulsion, space technologies, quantum technologies, biotechnologies, and novel materials and manufacturing (NMM).[35] The dependent variable of this study is "resilience." As it was presented in the literature review, resilience is defined at the most basic level as the ability to anticipate and withstand a disruptive event and quickly recover. This paper mirrors its definition of resilience after the United States' Department of Homeland Security concept of Relentless Resilience which "recognizes absolute prevention's futility but limits the damage of attack by nefarious actors or disasters through persistent preparation, response, and rapid

[35] NATO Science & Technology Organization, "Science & Technology Trends 2023-2043".

recovery."[36] This paper makes an original contribution to the literature on resilience as aims to make the case for resilience as a form of deterrence. While deterrence and resilience have typically



been defined separately, as seen by NATO's writing on resilience, this paper views resilience as a form of deterrence by denial. By increasing a state's resilience, it signals to any potential adversary that attacks would be fruitless, lengthy, and costly. Thus, this paper will study EDT's impact on the resilience of small, smart powers not only by how the small, smart powers innovate and incorporate EDT to become more resilient but also the deterrent effect of increasing such resilience. The complete model of this thesis with causal mechanism revealing how small, smart powers harness EDT and increase their resilience can be seen below:

[36]James Redick and Glenn Jones, *The Need for an Integrated Strategy: Denial, Deterrence, and Relentless Resilience* (North American Aerospace Defense Command, 2021).

The causal mechanisms linking EDT to resilience operate through three primary pathways. First, EDT adoption directly enables new defensive capabilities, creates deterrent effects, and enhances response capacity through technological integration. Second, institutional transformation occurs as small powers develop innovative cultures, create adaptive organizational structures, and integrate civilian-military capabilities. Third, strategic adaptation takes place as small powers implement asymmetric approaches, develop cost-effective defense solutions, and enhance hybrid warfare resistance. The key intervening variables in this process include innovation culture development, institutional adaptation capacity, civil-military integration, and strategic learning ability. These mechanisms and variables provide the framework for testing the main hypothesis: EDT integration increases resilience by spreading through the pathways of the *Small, Smart Power Model*.

Methodology

In trying to determine the relationship between small powers, EDT, and resilience, this thesis will employ process tracing as its research method. Process tracing provides a structure through which the thesis will identify the causal relationship between the independent and the dependent variables. By applying a process tracing method, the thesis will ground its inferences within each individual case. The thesis will specifically use a theory testing form of process tracing to prove the small, smart power model. Through theory testing, the paper will first test the model itself. From this point, the thesis will investigate the effect of EDT on the resilience of small, smart powers.

The thesis will test the model and its causal pathways against three qualitative cases studies: Ukraine, Estonia, and Singapore. The thesis has deliberately chosen a wide variety of cases

not only to distill the similarities between the cases but also understand the differences between small powers. Thus, the thesis has chosen cases that vary in geographical location, regime type, economy, and technological specialty. In doing so, the thesis hopes to gain strong explanatory power by studying such diverse cases. Additionally, it aims to demonstrate that the small, smart power model reflects a vast diversity of small powers. This approach may reveal that the attainment of small, smart power status is not limited to specific starting conditions or constraints and therefore provide external validity. As for the data collected on these cases, it will come from three sources. The first source of data comes from interviews conducted with European diplomats, European Parliament officials, NATO officials, think tank experts, scholars, and private sector officials that took place during the first two weeks of January. The second method of data collection will study official statements from politicians and national governments. The final source of data will be secondary reference sources to collect background on each case while also monitoring developments over time through think tank analysis, policy papers, and scholarly debate.

Turning to the three cases, the thesis will first look at Ukraine as an Eastern European power that has transitioned from a post-Soviet state to a decentralized, digital state that is rapidly transforming under wartime conditions. Its wartime experience provides real-time analysis of how EDT enhances resilience when facing an existential threat. Second, the thesis will study Estonia as a Northern European state that has also grew out from a post-Soviet state and is now an expert in digital services and e-governance. Through its focus on cyber capabilities and e-governance, Estonia manifests the ability for a small power to commit to bold, unconventional policies and unique technological advancements to increase its strategic position. Its membership of NATO and the European Union also provides a story of how small powers can develop technological

autonomy within larger alliances. Third, this paper will engage with the rise of Singapore as a Southeast Asian city-state, which has transformed from a colonial state to a global powerhouse and smart city leader. Singapore offers a challenge to the classic assumptions about small power limitations as it represents a state that has achieved technological, industrial, and military development despite its size. Singapore has become a global hub with one of the most advanced, technologically capable, and innovative armies in Southeast Asia.

Thus, this paper will apply theory-testing process tracing to test the causal forces within each part of the model and through the interlocking parts explain the specific output of resilience.

Chapter IV: Ukraine

Introduction:

The following case study will explore Ukraine as a living and breathing example of a small power fighting for its survival against a revisionist, threatening, aggressive great(er) power in Russia. Ukraine has exemplified the strength and resolve small powers hold when their survival is threatened. Ukraine has demonstrated that when small powers are faced with the necessity to survive, they are driven by innovation. While particularly apparent in the last four years of the invasion but existing for years before, Ukraine's technology ecosystem has become its greatest weapon. Starting with its realization of its dependence on Russia, Ukraine has fought to become self-sufficient and thus decentralize its institutions. In combination with decentralization, Ukraine pursued aggressive digitalization to streamline government processes, regain public trust, and eliminate corruption that was preventing development. As a result of decentralizing and digitalizing, Ukraine has created a model where the nation's survival is based on a total defense strategy. This total defense strategy pushes technological innovation as the lifeline through which all of Ukrainian society contributes to state survival. In positioning the whole of society towards defending the state, Ukraine has increased its resilience and survived, proving many speculators wrong.

What Makes Ukraine Small?

Given the comparative cases of Estonia and Singapore presented in this thesis, it may seem counterintuitive to consider Ukraine a small power. Smallness, however, is not just focused on landmass and population but is a relational concept that focuses on relative power, geographical position, and vulnerability within a state's regional and global position. Despite being the largest

country in Europe and ranking among the top ten most populous European states, Ukraine is still a small power. Since its independence in 1991, Ukraine has faced challenges projecting power and shaping the environment of its neighborhood. Instead of being directive, Ukraine has found itself reacting to actions of players in its region, unable to establish deterrence against Russian aggression and failing to gain full entry into the European Union or NATO. As a result, Ukraine has not been able to fully ensure its own survival without some external material and political support, whether that has come from Western aid, NATO, EU trade agreements, or foreign direct investment. The annexation of Crimea in 2014, ongoing fighting in the Donbas region from 2014 until 2022, and the full-scale invasion starting in 2022 have all revealed the limits of Ukraine's conventional military capabilities and its geographic vulnerabilities, specifically coming from its eastern border with Russia. These vulnerabilities have been connected to Ukraine's geographic conditions. Lodged between Europe and Russia, Ukraine has attempted to survive in this contested zone of great power influence. Its geography does not bolster security, but instead inflames exposure as it has been vulnerable to invasion from all fronts and has been forced to adapt.

Thus, beyond the absolute metrics of smallness, Ukraine, like Estonia and Singapore, has struggled with the conditions of limited regional influence, external dependencies, and deep security vulnerabilities that reinforce smallness. To compensate for its smallness, Ukraine has pursued innovation, societal mobilization, and unconventional strategies. This renewed identity has enabled Ukraine to transform these structural constraints into sources of smartness and resilience.

Smallness Growing into Smartness:

Post-Soviet Turbulence

Following the collapse of the Soviet Union in 1991, Ukraine began its journey of redefining itself as its own independent state. In the period between 1991 and 2014, Ukraine developed three main deficiencies. First, its political institutions rotted from within as they slowly lost the ability to mobilize political leadership and the public. Second, Ukraine failed to build sufficient defensive capabilities to fight back against threatening adversaries. Finally, Ukraine lacked a set of shared values that would allow a unifying response to any security threats.

Left to rebuild its own political, economic, and institutional systems, Ukraine also had to devise a plan for its defense and security. Ukraine's security and defense industry, however, did not rise from the dust. Ukraine inherited nearly 30% of the Soviet Union's defense industry, which had been left within Ukraine's territory, including 750 factories, 140 scientific and technical institutions, and 1 million people employed by these various institutions.[37] Ukraine was handed a model where the state had almost total control over the defense industry. Over the next two decades after the dissolution of the Soviet Union, Ukraine continued to produce Soviet-style weapons. These weapons, however, began to lose their technological edge as other states began making more advanced weaponry and Ukraine's clients began looking at other producers. Ukraine made multiple attempts to privatize and modernize its defense industry but failed due to a lack of an incentive structure for industrial development, an inefficient asset structure, neglected human capital, and deep corruption and political interference. Absorbing less than 30% of the country's total defense industrial output while exporting nearly $1.3 billion of defense-related products in

[37] Alexandra McLees and Eugene Rumer, "Saving Ukraine's Defense Industry," Carnegie Endowment for International Peace, July 30, 2014, https://carnegieendowment.org/research/2014/07/saving-ukraines-defense-industry?lang=en.

2014, Ukraine's own military was not large enough to sustain its oversized defense industry.[38] Additionally, economic contraction throughout the 2000s prevented technological advancement from taking place. This led the surviving defense companies, who could no longer compete in the global arms market, to become increasingly dependent on a small group of buyers to stay afloat. Thus, the Ukrainian defense industry became even more dependent on exports.

Of all its customers, one specifically stood out: Russia. From 2009 to 2013, Russia was the third largest buyer of Ukrainian defense products only behind China and Pakistan.[39] As Ukraine became more dependent on Russian contracts, the relationship between the Ukrainian and Russian defense industries became more ingrained. Russia was dependent on certain parts and services which it solely imported from Ukraine. Russia's military depended on Motor Sich for its helicopter engines produced in the Ukrainian city of Zaporizhia.[40] The Russian army depended on Yuzhmash, or the Machine Building Plant Association, in the Ukrainian city of Dnipropetrovsk to design, produce, and repair rockets and missiles.[41] More than half of the parts needed for Russia's ground-based intercontinental ballistic missiles came from Ukraine as well.[42] At the same time that Ukraine depended on exports to Russia and Russia depended on Ukraine, Ukraine also depended on Russia for imports.

Ukraine's inability to separate itself from its main adversary derived from a greater systemic problem reflected in the national security strategies of the nation's presidents. Both Viktor Yushchenko's 2007 national security strategy and Viktor Yanukovych's amended strategy in 2012 lacked a direct articulation of precise threats to Ukraine and, more concerningly, failed to entertain

[38] Ibid.
[39] Siemon T. Wezeman and Sam Perlo-Freeman, "The Ukraine Conflict and Its Implications: III. The Impact of the Crisis in Ukraine on Arms Transfers," in *SIPRI Yearbook 2015 : Armaments, Disarmament and International Security* (World Armaments And Disarmament Oxford: Oxford University Press, 2015), 86–98.
[40] Alexandra McLees and Eugene Rumer, "Saving Ukraine's Defense Industry."
[41] Ibid.
[42] Ibid.

any possibility of Russian aggression.[43] It was written that Ukraine had an "undemarcated border" with Russia, Moldova, and Belarus without any consideration of what such a statement might imply for Ukraine's integrity.[44] Yanukovych's national security strategy further proposed a "strategic partnership" model with Russia that included a "search for common approaches to forming an all-European collective security system."[45] The document commented on the poor state of the Ukrainian Armed Forces (UAF) and defense industry yet presented no policy or strategy to reverse the worsening trend or measure the effectiveness of reform. The UAF were consistently downsized, and military equipment was sold off.[46] To complement this trend, defense spending remained under 1% of GDP annually, preventing any modernization of military equipment or increased training of forces.[47] The UAF were bled out so extensively that, when Ukraine faced the covert and overt attacks by Russia in 2014, the Ukrainian defense minister barely had 7,000 combat-ready troops under his command.[48] The damage of this depletion was multiplied by a mass defection of Ukrainian soldiers to the Russian side when 75 % of Ukrainian personnel switched to the Russian side in March 2014.[49] The total Ukrainian military had shrunk from 800,000 personnel in 1991 to 130,000 by 2014.[50] Not only did the Ukrainian government actively weaken its security and defense muscle, but the country's own soldiers held no commitment to the state nor trust in national leadership.

[43] Serhiy Kudelia, "The Ukrainian State under Russian Aggression," *Current History* 121, no. 837 (October 1, 2022): 251–57, https://doi.org/10.1525/curh.2022.121.837.251, 253.
[44] Ibid. 253.
[45] Ibid. 253.
[46] Paul Holtom, "Ukrainian Arms Supplies to Sub-Saharan Africa," *Stockholm International Peace Research Institute*, February 2011, 1–16, https://www.sipri.org/sites/default/files/files/misc/SIPRIBP1102.pdf.
[47] Kudelia, "The Ukrainian State under Russian Aggression," 254.
[48] Adrian Bonenberger, "Ukraine's Military Pulled Itself out of the Ruins of 2014," Foreign Policy, May 9, 2022, https://foreignpolicy.com/2022/05/09/ukraine-military-2014-russia-us-training/.
[49] Kudelia, "The Ukrainian State under Russian Aggression," 254.
[50] Bonenberger, "Ukraine's Military Pulled Itself".

Politically, the country split across regional cleavages. Since 2004, voters split between the southern-eastern bloc that opposed the western bloc. The western block of Ukraine became the pro-Western, or "Orange," sect while the southern and eastern bloc became the pro-Russian, or "Blue," sect. These divisions were deeply rooted in the demographic spread of ethnic divisions across Ukraine, which formed regional identities. In Donbas and Crimea, a large ethnically Russian-speaking minority supported an economic and political union with Moscow, while the west wanted to join Western institutions like NATO and the EU. In August 2023, a rating poll recorded that 57 percent of Donbas residents fully or partially opposed Ukraine's independent statehood.[51] This ethnic and linguistic divide hurt Ukraine's attempts at forging an unified national identity.

Catalyzation: Euromaidan Revolution and the Annexation of Crimea

The combined effects of the Euromaidan Revolution and Russia's annexation of Crimea in 2014 forced Ukraine to confront two existential crises: its corrupt, rotten institutions had failed Ukrainians, and its military-industrial system could not guarantee the nation's sovereignty. The Maidan Revolution, or Revolution of Dignity as it is also known, revealed the corruption, lack of accountability, and authoritarianism that had developed in Ukraine since its independence. By 2013, Ukraine ranked 144 of 177 in the Transparency International Corruption Perception Index and was estimated by the World Bank to be losing 60 billion Ukraine hryvnia (UAH) or $2.2 billion annually due to corruption.[52] The pro-Russian president at the time Viktor Yanukovych also represented the rot that had taken place within Ukraine with his ostrich farm and golden toilets,

[51] Kudelia, "The Ukrainian State under Russian Aggression," 255.
[52] George Ingram and Priya Vora, "Ukraine: Digital Resilience in a Time of War," Brookings Institute, January 30, 2024, https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/.

which he housed in his presidential palace.[53] When Yanukovych abruptly decided to reject the EU Association Agreement that would bring Ukraine closer to EU accession in favor of closer Russian ties in November 2013, Ukrainians took to the streets across the country, protested, died, and ousted Yanukovych by February 2014. After an brief interim government, Petro Poroshenko took office in May 2014, and Ukrainians planted the seeds for citizen-led state-building.

Directly after the Maidan revolution, Vladimir Putin sent Russia military forces into Crimea in February 2014 and seized control of the region. Shortly afterwards, fighting broke out in the Donbas region between Russian-backed forces and the Ukrainian military which would last for years and escalate with the 2022 full-scale invasion. The military confrontations revealed that Ukraine lacked a coherent military posture, had a weak military, and was deeply entangled with its greatest adversary. As a matter of fact, the United Operational Commands of Ukraine, which served as support to protect the north-eastern side of the nation, had been completely and intentionally disbanded by Yanukovych between 2010 to 2013.[54] The annexation of Crimea was deeply terrifying and humiliating for Ukraine. It represented an escalation of Russian aggression that moved beyond diplomatic and economic realms to a kinetic, military level. In the face of this escalation, the UAF had proven to be completely inept, and Ukraine had completely failed to defend itself it.

The Maidan revolution and annexation of Crimea presented Ukraine with a critical juncture.[55] The old political institution and tradition of remaining in the Russian orbit were exposed

[53] Tymofii Brik and Jennifer Brick Murtazashvili, "The Source of Ukraine's Resilience: How Decentralized Government Brought the Country Together," Foreign Affairs, June 28, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-06-28/source-ukraines-resilience.
[54] Sergii Glebov and Denys Kuzmin, "On the Way to Ukraine's Total Defence System," in *European Total Defence: Past, Present, and Future*, ed. Gjermund Forfang Rongved (London: Routledge, 2025), https://doi.org/10.4324/9781003497370-2, 21.
[55] Robert Lumack, "Defence and Military Reform in Ukraine 2014-2022" (2025), https://doi.org/10.20381/ruor-30833,121.

as inadequate and lost total legitimacy. With the structural constraint of Yanukovych gone, Ukrainian society had a full range of possibilities to innovate and reform. This opening of options to reform the Ukrainian state and society was also reflected in the military. This critical juncture was taken in full stride by Ukrainian society who shed their institutions of their Soviet chains and implemented radical change.

In response to the annexation of Crimea, civil society did not remain passive. Instead, it started defending the state directly. Just as the Maidan revolution had sparked civil society into fighting for its interests, the annexation of Crimea raised the defense of Ukraine into a total society undertaking, blurring the lines between civilian and defense actors. What started as a democratic revolution with the Maidan revolution evolved into a national defense uprising after the annexation of Crimea.

As will be shown in the following sections, these two events planted the seeds for Ukraine's total defense approach. Under Petro Poroshenko's leadership, Ukrainians were given full control and reformed the state and society from the bottom up. This comprehensive society-based approach to reforming the state spread to the reform of the Ukrainian defense apparatus as Ukraine began forming a total defense approach. Volunteers aided the weak Ukrainian military, crowdfunding campaigns were launched, and private actors developed technology. In the aftermath of the dual shocks, Ukraine began its transformation toward becoming *smart* through full societal mobilization, security reform, and technological innovation. Ukrainians did not wait for institutions to rebuild; society mobilized from below to defend its future. The Ukrainian decision across state, society, and military in 2014 to fight, reform, and resist laid the groundwork for their ultimate decision to fight in 2022.

Planting the Seeds of Smartness–Decentralization

Following 2014, Ukraine used decentralization as a political and administrative philosophy and digitalization as the technical means to reform and modernize society. The newly elected Petro Poroshenko and his new administration were motivated to urgently rid Ukraine of its internal rot in order to counter threats from Russia and regain the trust of Ukrainians. Similar to the story of Estonia, Poroshenko focused on rebuilding Ukrainian society by creating transparency, fighting corruption, placing power in the hands of the people, and regaining trust.

Decentralization was not a new phenomenon when implemented by Poroshenko. It had been discussed as a new possibility for structural reform since 1991 and was attempted by Viktor Yushchenko twice in 2005 and 2009. While the first time decentralization was drawn up by then vice prime minister of the time, Roman Bezsmertnyi, it was abandoned after his resignation.[56] In 2009, the plan was abandoned again due to the transition to the Yanukovych government as it was said, *"While the draft of 2005 got lost somewhere in the Prime Minister's drawer, the document of 2009 disappeared in the maze of the Cabinet's Secretariat."*[57] It was not until 2014 under Poroshenko that decentralization was pursued as the plan that could make Ukraine balanced and sustainable. Following the Maidan revolutions which spread beyond the central square in Kyiv across cities in all regions of Ukraine, citizens called for a government that was more responsive to its people and an end to Ukraine's entrenched corruption. This call was met by Poroshenko and a new generation of politicians who pushed reforms based on the need for more transparent,

[56] William Dudley, "Ukraine's Decentralization Reforms," *Stiftung Wissenschaft Und Politik (SWP)* 1 (May 2019): 1–34, https://www.swp-berlin.org/publications/products/arbeitspapiere/Ukraine_Decentralization_Dudley.pdf.
[57] Anatoliy Tkachuk, "Decentralization, Progress, Risks and Role of the Ukrainian Parliament - Інститут громадянського суспільства," Dzerkalo Tyzhnia, January 13, 2017, https://www.csi.org.ua/news/decentralization-progress-risks-role-ukrainian-parliament/.

decentralized, and accountable government processes. Instead of decentralizing from the top down, these politicians chose a bottom-up process.

Poroshenko introduced two defining concepts almost immediately: the "Concept of Reforming Local Self-Government and Territorial Structure of Power" approved by the Cabinet of Ministers in April 2014 and the "State Strategy for Regional Development 2015-2020" approved in August 2014. Through these reforms, Poroshenko first addressed the concept of subsidiarity.[58] In 2014, Ukraine consisted of 24 oblasts, or regions containing between 1 to 2 million people, the republic of Crimea, 2 cities with special oblast status in Kyiv and Sevastopol, 490 Rayons or districts with around 50,000 people, 11,518 communities, and 176 cities that were recognized as "Cities of Oblast Significance" that were collectively to nearly 20 million people.[59] Under this categorization of Ukraine, the government follow a four tiered hierarchy starting at with the central government, then oblast, then rayon, and ending with village and communities. At the oblast and rayon levels, power was shared between the state administrator who was appointed by the central government and the locally elected councilors. Not only was the system overly complicated, but it was also being taken advantage of. The state administrators held control over executive authority and made the majority of decision. They remained unaccountable to anyone but the central state administration which appointed them. Spreading corruption, they hindered economic growth and hurt public services as they disregarded local demands and funneled money into. Thus, local Ukrainians had no voice to fight back with, and local government administrations lacked the capacity and budgets to push back since they depended on transfers from the corrupt

[58] Olga Oleinikova, "Decentralization Reform: An Effective Vehicle for Modernization and Democratization in Ukraine?," in *Decentralization, Regional Diversity, and Conflict*, ed. Hanna Shelest and Maryna Rabinovych (Cham: Springer International Publishing, 2020), 311–38, https://doi.org/10.1007/978-3-030-41765-9_11.
[59] Dudley, "Ukraine's Decentralization Reforms".

central officials.[60] By creating clear levels of self-governance with clear mandates of authority and financial power, Poroshenko attempted to create economic stability by decentralizing government. He gave power back to local authorities who cared about improving the communities. Revenue no longer flowed directly to the central government. Instead, it was said that, after reforms, 60% of local revenue stayed at the local level.[61] With local authorities retaining growing resources and holding decision making power, they used the new funds productively on infrastructure and community welfare. Subsidiarity reduced inefficiency and corruption as local authorities now responded directly to the desires of their electorate.

Poroshenko's other major decentralization reform was to propose the concept of amalgamation. Through the 2015 Law of Ukraine "On Voluntary Amalgamation of Territorial Communities" (ATCs), Poroshenko gave local communities the option to self-organize and join into larger local governmental units known as *hromadas*.[62] Poroshenko believed that forming an integrated community would generate larger, innovative projects by pooling together greater cultural, social, and economic resources for development. While not all towns and villages formed *hromadas* after the law went into effect in 2016, by 2019 4,018 formal local councils had merged and 878 ATCs had been established.[63] Having willingly joined to form larger local governments that collected higher tax revenues based on self-government, community ties were bolstered. The amalgamation reform also spoke profoundly to Ukrainian identity.[64] Ukrainian society has long been suspicious of authority and hierarchy. Ukrainians have self-organized to solve problems

[60] Lily Salloum Lindegaard and Neil Anthony Webster, "Supporting Political Stability by Strengthening Local Government: Decentralisation in Ukraine," *Danish Institute for Interational Studies* 2018, no. 7 (May 28, 2018): 1–96, https://pure.diis.dk/ws/files/2543996/DIIS_Report_07_Ukraine_WEB.pdf, 23.
[61] Brik and Murtazashvili, "The Source of Ukraine's Resilience".
[62] Oleinikova, "Decentralization Reform".
[63] Ibid.
[64] Volodymyr Yermolenko, "Ukraine's Resilience and Why It Continues to Fight," Chatham House, February 8, 2023, https://www.chathamhouse.org/2023/02/ukraines-resilience-and-why-it-continues-fight.

through *toloka*, or a community effort to solve shared problems.[65] Thus, amalgamation reform strengthened Ukrainian identity and unified citizens. Ukrainians were given the power to decide how to structure their own institutions from the bottom up and decide to unify together.

Thus, the decentralization reforms starting in 2014 formed a new base of political legitimacy and collective action. Paradoxically, Ukraine strengthened its state by devolving power. This devolution of power had "transformed zero-sum ethnic competition into positive-sum community pride."[66] Both Ukrainians and native-speaking Russians held a stronger sense of devotion to their government as they felt responsible for building their country. Increased pride and satisfaction with local government only produced more support for reform. In a survey**,** 19% of respondents claimed their lives improved because decentralization; however, this number jumped to 59% by 2020.[67] Additionally, Ukrainians regained trust in local elections as voting became consequential and increased accountability of local officials. Hence, decentralization created a responsive, citizen focused governance structure through the lived experience of reform.

Planting the Seeds of Smartness–Digitalization

Parallel to decentralization, digitalization created a network to connect this new Ukrainian society, reinforcing trust, improving services, and countering corruption. While Ukraine's digital transformation began in 2012 under the guidance of the Organization for Security and Cooperation in Europe (OSCE) and the eGovernment Academy (eGA) of Estonia, Poroshenko began building the main architecture for Ukraine's e-government systems starting in 2014 with help from various

[65] Anastasiia Kudlenko, "Roots of Ukrainian Resilience and the Agency of Ukrainian Society before and after Russia's Full-Scale Invasion," *Contemporary Security Policy* 44, no. 4 (September 20, 2023): 1–17, https://doi.org/10.1080/13523260.2023.2258620, 521.
[66] Yahya Alshamy et al., "Polycentric Defense, Ukraine Style: Explaining Ukrainian Resilience against Invasion," *Journal of Public Finance and Public Choice* 39, no. 1 (April 17, 2023): 36–58, https://doi.org/10.1332/251569121x16795569226712, 38.
[67] Brik and Murtazashvili, "The Source of Ukraine's Resilience".

actors and organizations like SIDA, USAID, UKAID, UNDP, and the Estonian government. Poroshenko's first step was to transform the Center for E-government into an independent agency known as the Agency for E-governance.[68] This agency worked with individual ministries to oversee the digitalization of agencies; however, an institutional problem existed since the Agency for E-governance did not have the authority to control the approaches of ministries.

Digitalization policy matched the transparency initiatives of decentralization reform by passing complementary laws. In 2014, *Verkhovna Rada*, the common name for the Ukrainian Parliament, passed a law on asset declaration which required all government employees to declare their assets.[69] This was followed in 2016 by the passing of a law on public procurement that enacted effective, transparent mechanisms for public procurement, created a competitive culture, and eliminated corruption risks.[70] In 2018, Cabinet Decree 357 on state electronic information resources created a singular interoperable system of public registries, known as Trembita, to enable seamless e-government services and prevent registries from being duplicated.[71]

Two key e-government instruments were introduced during Poroshenko's presidency: ProZorro and the aforementioned Trembita. ProZorro, which translates to transparency, was launched in 2015 as an e-procurement platform to make government procurement efficient and transparent.[72] Created by private-public industry collaboration with 300 volunteers and support from the Ministry of Economy, the platform aimed to eliminate the human elements in the

[68] Ingram and Vora, "Ukraine: Digital Resilience," 7.
[69] Nicholas Nam, "Reform of Asset and Interest Disclosure in Ukraine," *World Bank Group*, January 16, 2021, 232–37, https://thedocs.worldbank.org/en/doc/457791611679267058-0090022021/original/ReformofAssetandInterestDisclosureinUkraine.pdf.
[70] Ingram and Vora, "Ukraine: Digital Resilience," 7.
[71] Ibid.
[72] Ingram and Vora, "Ukraine: Digital Resilience," 7.

procurement process that lead to corruption.[73] ProZorro soon became the standard central system for the entire procurement process ranging from collecting tender notices, submitting and reviewing bids, and awarding contracts. ProZorro was created on three principles. First, ProZorro was built entirely through open-source code, allowing for open data, open publishing, and open standards. Second, ProZorro emphasized transparency, making all data, including actors, tender notices, bids, contract awards, and qualification documents publicly available to all agencies, civil society organizations, and media. Finally, ProZorro aimed to complete the golden triangle partnership between the state, businesses, and civil society to split functions between stakeholders while increasing accountability. Built on transparency, ProZorro served as a watchdog accountability mechanism to monitor and expose all procurement.

Complementing ProZorro, Trembita was launched in 2018 as a digital interoperable data exchange system. While modeled closely after Estonia's X-Road system, Trembita differed by transforming global best practices to meet Ukraine's needs and using cryptography standards that conform to Ukrainian regulation. Ukraine had tried to adopt Estonia's open-source code for X-Road but instead licensed the Estonian company Cybernetica to use its Unified Exchange Platform to build Trembita.[74] Trembita serves as a digital nervous system for Ukraine, enabling rapid data exchange and communication between citizens and various levels of government. Trembita is secure since officials cannot see individuals' data, all data is encrypted during transmission and storage, and any data entered or modified is signed with a digital signature and registered. Rather

[73] Olexandr Starodubtsev, *YOUkraine. Because ProZorro.* (World Bank, 2015), https://thedocs.worldbank.org/en/doc/828301490813177880-0310022017/original/UseofeGPforopenDataOlexandr.pdf.
[74] Cybernetica, "Secure Data Exchange & Interoperability," Cyber.ee, 2025, https://cyber.ee/products/secure-data-exchange/.

than centralizing data in a single space, Trembita decentralized down to the level of peer-to-peer exchange, reducing opacity and increasing trust in government.

Following a period of anti-corruption and digital government reforms under Poroshenko, the election of Volodymyr Zelenskyy completed Ukraine's transition towards full e-governance. Having campaigned on "a state in a smartphone" platform," Zelenskyy set out to build a convenient digital administrative state that minimized bureaucratic government red tape which opened opportunities for corruption.[75] Elected in 2019, Zelenskyy created the Ministry of Digital Transformation in the same year. Rather than appointing a veteran politician, Zelenskyy appointed his Deputy Prime Minister Mykhailo Fedorov, who was a young start-up entrepreneur, as Minister of Digital Transformation. Zelenskyy used Estonia as a model and advisor, embedding 30 Estonian advisers within the Ministry of Digital Transformation.[76] The creation of the ministry served as a credible commitment from Zelenskyy to Ukraine's digital transformation. The ministry itself was set up to oversee the digital development across Ukraine's ministries and agencies but lacks the power to institute specific changes.

To compensate for this lack of power, Zelenskyy also created a network of Chief Digital Transformation Officers (CDTOs) for every ministry who held the power of a deputy minister. With each CDTO responsible for overseeing the digital transformation of each agency at the central, regional, and local level, Zelenskyy followed the trend of decentralization and shifted the impetus for reform away from a single ministry or political appointee. This strategy proved successful as of mid-2023 with 15 CDTOs spread across the 24 oblasts and a plan to add an individual CDTO to the more than 1400 municipalities.[77] Each CTDO at the local and community

[75] Gulsanna Mamediieva and Donald P Moynihan, "Digital Resilience in Wartime: The Case of Ukraine," *Public Administration Review* 83, no. 6 (October 22, 2023): 1512–16, https://doi.org/10.1111/puar.13742.
[76] Ingram and Vora, "Ukraine: Digital Resilience," 3.
[77] Ingram and Vora, "Ukraine: Digital Resilience," 10.

level oversees the integration and protection of critical infrastructure, the dispersion of electronic services, the spread of internet, and the increase of digital literacy.

Perhaps Zelenskyy's greatest achievement was the creation of the Diia app. Diia, which means "action" and also an acronym for "the state and me," was introduced in 2020. It included a mobile application and web portal built on the Trembita system that enabled easy, centralized citizen government interactions. While the mobile app started by collecting digital documents and public services, the government web portal offered public services, education projects for the development of digital skills and literacy projects to facilitate small and medium-sized enterprise growth and innovation. The app was built with the goal of reducing administrative burdens placed on citizens and businesses in order to allow Ukraine to rapidly develop.

For citizens, Diia offers services like applications for housing loans, submitting tax declarations, paying taxes, COVID-19 vaccination waiting list, and application for financial assistance. The app hosts more than 25 public services while the government web portal offered over 90.[78] It grants citizens mobile access to digital versions of basic documents: national ID cards, passports, student ID, driver's license, vehicle registration certificates, vehicle insurance policy, tax numbers, and migrant certificates. Through Diia, Ukraine became the first country in the world to create a digital passport and the fourth in Europe to have a digital driver's license. For businesses, Diia.Business offers a one-stop-shop for entrepreneurs. With easy registration, Diia.Business offers free consultations and training on about 70 topics, like legal advice, taxation, finance, human resources, marketing, and access to financial support programs. Other Diia spin-offs like Diia.Engine and Diia.City has also proven to be vastly popular, offering unique, innovative frameworks to empower Ukrainians. Diia's success is proven by the number of its

[78] Mamediieva and Moynihan, "Digital Resilience in Wartime."

users. Nearly 19 million Ukrainians use the Diia mobile app, and nearly 22 million Ukrainians use the Diia web portal out of a total adult population of 33 million people.[79] Thus, digitalization has worked in coordination to modernize Ukraine's state infrastructure and streamlined citizen access to services. More importantly, it has empowered a shared digital identity, uniting communities under a common framework based on trust, transparency, and active engagement, therefore reinforcing societal strength and unity.

Modernization as a Spark: From Reform to Resilience through Total Defense

Following the Euromaidan and the invasion of Crimea, Ukraine fought to bolster its own defense. Ukraine laid the groundwork starting in 2014 for the flourishing of total defense by 2022. Through the leadership of Poroshenko and Zelenskyy, Ukraine expanded its definition of defense beyond simply military defense to a whole-of-society Total Defense strategy. Both leaders worked to strengthen national identity as a base to include all Ukrainians in the preparation for any possible threat the nation might face. Increasing Ukraine's security stretched beyond rebuilding defunct military industrial capacities, reorganizing military structure, and increasing the size of forces. The ongoing fight against Russian separatists in the Donbas furthered national unity and sparked a rise in civilian volunteers taking it upon themselves to fight for their country. The existential threat Russia posed, as well as the new style of hybrid war which Ukraine now faced, sparked a push toward defense that engaged all sides of society and required all Ukrainians to participate.

In 2014, Poroshenko placed a ban on all military-technological cooperation with Russia. This was supported by a statement from Yuriy Tereshchenko, the head of Ukroboronprom at the

[79] Ibid.

time, who halted all exports of weaponry and equipment to Russia.[80] Ukroboronprom was the state-holding company established in 2010 that oversaw 134 Ukrainian state-owned defense companies and employed 120,000 workers in total at the time.[81] Ukroboronprom serves as a perfect example of the change that needed to occur within Ukraine. Ukraine's defense sector was a living contradiction. Ukraine had a defense sector that was entirely state-controlled yet simultaneously lacked control over the entire defense industry with regulatory licensing and export control functions scattered across multiple government agencies and ministries. Additionally, its biggest partner was Ukraine's biggest enemy: Russia. Despite the catastrophic results of such a ban, causing the collapse of Ukrainian defense companies and unemployment levels which had not been since the collapse of the Soviet Union, Poroshenko followed through.[82] The ban was not simply an economic decision but a strategic move to separate Ukraine from its dependency on its enemy. The ban broke Ukraine's defense industry from the shackles of its technologically backwards Soviet past and forced open a new innovative path for light to shine through.

Implementing policies to break all ties from Russia, Ukraine introduce the Resistance Operating Concept (ROC) as a new basis for an unconventional strategiy that used the newly empowered civilian society of Ukraine to commit all resources towards a whole-of-society defense. ROC was developed by the United States in 2013 following Russia's invasion of Georgia as a blueprint for smaller powers to resist and confront larger neighbors if invaded.[83] Ukraine was the first state to adopt the concept as its national strategy. Ukraine used ROC as an innovative unconventional method for war and total defense that required both the military and the whole of

[80] Katya Gorchinskaya, "Ukroboronprom Director Says Weapons Shipments to Russia Stopped Three Weeks Ago," Kyiv Post, April 15, 2014, https://www.kyivpost.com/post/10033.
[81] McLees and Rumer, "Saving Ukraine's Defense Industry".
[82] Gorchinskaya, "Ukroboronprom Director Says Weapons".
[83] Oren Liebermann, "How Ukraine Is Using Resistance Warfare Developed by the US to Fight Back against Russia," CNN, August 27, 2022, https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

society. In Ukraine, ROC was conceptualized as an unconventional, asymmetric approach to war based on small, mobile military units that used guerilla tactics to fight a conventionally armed force. These units would be supported by the whole population as they contribute, produce, and innovate in order to increase the asymmetric capabilities of their defense. The introduction of ROC led to a "deterrence-resilience-cooperation" framework to support Ukraine's total defense. The strategy was reaffirmed by NATO which stated that resilience is "the first line of deterrence and defense."[84] This resilience is based on close civil-military cooperation conceptualized in the 2020 National Security Strategy called "Human Security – the State's Security."[85] The strategy outlined deterrence as the development of capabilities to prevent attacks against Ukraine; resilience as society's ability to react, adapt, and respond to the changing security environment; and cooperation as strengthening ties within society and with international partners to bolster Ukrainian national security. This "deterrence-resilience-cooperation" concept bonded civil-military cooperation together, consecrated by the concept of resilience.

Under President Poroshenko, Ukraine reorganized its defense sector, utilizing its smart digital networks to bolster Ukrainian defense. The defense sector became a critical juncture for reshaping control, cutting off Russian dependencies, and collaborating with private tech partnerships. The strategic aim was clear. Ukraine needed a defense ecosystem that could survive independently, modernize rapidly, and adapt to the fast pace of war— the foundations of a smart, resilient security state. As was previously mentioned, ProZorro played a vital role in reforming the government procurement process. ProZorro was created by a group of civil society volunteers, symbolizing the commitment of Ukrainians to improve the nation from the bottom up. In its first

[84] NATO, "Deterrence and Defence," NATO, December 10, 2023, https://www.nato.int/cps/en/natohq/topics_133127.htm.
[85] Glebov and Kuzmin, "On the Way to Ukraine's Total Defence System," 28.

five years of use, ProZorro saved nearly $7 billion for private companies working through the government contract procurement process.[86] The increased ease of procurement, lower costs, and simplification of bureaucratic hurdles increased participation from the private sector. The financial incentives and easier process also combined with the passionate civil society that was committed to taking part in the defense of Ukraine. As a result, start-ups began emerging as well as new dual-use technologies were introduced by established private sector companies. These companies made major strides in EDT like situational awareness systems and drone technology. From 2014 to 2022, Ukraine's patriotic, tech-savvy workforce introduced 11 new situational awareness and battlefield management systems to the UAF.[87] These systems included fire control, artillery optimization, air traffic management, and combat command and control. The Army SOS volunteer group developed the Kropyya artillery software that allows artillerymen to use a tablet or a phone to enter enemy coordinates and fire from the closest artillery battery with precalculated aiming trajectories. This system has improved target accuracy and reduced the time between receiving orders and striking by tenfold.[88] This volunteer driven innovation has been so successful that 90 to 95% of Ukrainian artillery units use it as their primary fire control system.[89] Another innovation is GisArta, which has been labelled the "Uber for artillery," using a bottom-up approach to centralizing battlefield intelligence and producing target strike information.[90] By restructuring the defense industry, Ukraine opened new channels for a diverse set of Ukrainians to contribute towards defending the country. While some of these innovations began wide purely civilian purposes and others with the

[86] Ilan I. Berman and Matt Cesare, "Ukraine Reform Monitor No. 1," American Foreign Policy Council, June 29, 2023, https://www.afpc.org/publications/bulletins/ukraine-reform-monitor/ukraine-reform-monitor-no-1.
[87] Viktor Putrenko and Nataliia Pashynska, "Military Situation Awareness: Ukrainian Experience," *Applied Cybersecurity & Internet Governance* 3, no. 1 (July 17, 2024): 122–46, https://doi.org/10.60097/acig/190341.
[88] Kateryna Bondar, "Understanding the Military AI Ecosystem of Ukraine," Center for Strategic and International Studies, November 12, 2024, https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine.
[89] Bondar, "Understanding the Military AI Ecosystem of Ukraine".
[90] Mark Bruno, "'Uber for Artillery' - What Is Ukraine's GIS Arta System? - the Moloch," The Moloch, August 24, 2022, https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/.

direct aim of supporting warfighter decision-making, they have evolved into EDT platforms that are routinely used by hundreds of thousands of soldiers.

In addition to rebuilding technological military capabilities, there was also an imperative to rebuild the UAF. In response to the 2 catalysts and fighting in the Donbas region, Ukrainians committed to defending their state, and the number of active-duty soldiers saw an increase from 123,000 in 2014 to a standing army of 209,000 by 2021.[91] The ongoing fighting in the Donbas strengthened the total defense strategy as Ukrainians united to fight the Russian separatists. The Ukrainian government took a drastic step and authorized the formation of self-organized and self-funded militias. In response to this change, tens of thousands of Ukrainians joined volunteer militia groups, contributing to logistic operations and even joining the fight on the frontlines with Ukrainian soldiers. When asked about the experience of fighting Russia in the Donbas, Ukrainian civilians and soldiers claimed it was fundamental to "Ukraine's understanding of itself as a nation and for the military's understanding of its capabilities and deficiencies."[92] Ukrainians of all backgrounds joined volunteer groups and crowdsourcing campaigns in order to support the fight in the Donbas.

The rallying cry from Ukrainian citizens who volunteered and took up arms to fight together in the Donbas was so strong that Ukraine passed laws to expand participation in its armed forces. In August 2021, the law "on the foundations of national resistance" created the Territorial Defense Forces (TDF) as a stand-alone branch of the official military, made up solely of volunteers. The TDF comprises of 10,000 career positions with 120,000 civilian reservists organized into 20

[91] Richard Shimooka, "Towards a Better Integrated, Better Equipped Ukraine: Richard," Macdonald-Laurier Institute, February 16, 2024, https://macdonaldlaurier.ca/towards-a-better-integrated-better-equipped-ukraine/.
[92] Bonenberger, "Ukraine's Military Pulled Itself".

regional brigades.[93] Another interesting switch was the renaming of the "Anti-Terrorist Operation" (ATO), which the Ukrainian government had named the fighting in the Donbas in 2014, to the "Joint Forces Operation" in 2018.[94] The title ATO treated the threat to Ukraine as an internal problem that required rooting out separatists. It did not fully acknowledge that the real threat came from Russia. With the name change, the Ukrainian government included these forces into the National Guard of the Ministry of the Interior. It marked an official recognition of Ukraine's biggest threat as Russia and not domestic separatists. In doing so, Ukraine fought to reaffirm national unity. The conflict solidified the psychological part of total defense as it united Ukrainians and built a national identity. Ukrainians of Russian descent even reclassified their nationalities as Ukrainian as it was found that one in three Russian speakers reclassified between April to December of 2014.[95] Language use also changed as the number of sole or primary Russian language users dropped from 34.7% to 25.7% between 2014 and 2017.[96] The military and militias reformed their structures to be meritocratic and flat-structured, reflecting the influence of bottom-up principles based on national trust and unity. This new meritocratic military culture represented an innovative, operational concept that was unknown under the top-down, heavily centralized Soviet system.

While the fighting in the Donbas contributed to the formation of national Ukrainian identity, the government also implemented a series of policies to capitalize on the increasing Ukrainian national pride and reduce Russian influence. Broadcasts of Russian television were banned, Russian social media networks were blocked, Russian newspapers and films were banned,

---

[93] John Spencer and Liam Collins, "How Volunteers Can Help Defeat Great Powers," Military Times, July 5, 2022, https://www.militarytimes.com/opinion/commentary/2022/07/05/how-volunteers-can-defeat-great-powers/.
[94] Glebov and Kuzmin, "On the Way to Ukraine's Total Defence System," 22.
[95] John O'Loughlin and Gerard Toal, "Does War Change Geopolitical Attitudes? A Comparative Analysis of 2014 Surveys in Southeast Ukraine," *Problems of Post-Communism* 67, no. 3 (November 15, 2019): 303–18, https://doi.org/10.1080/10758216.2019.1672565, 308.
[96] Kudelia, "The Ukrainian State under Russian Aggression," 255.

and Russian language education was severely restricted. The government decommunized Ukraine, removing over 1,000 Lenin and Soviet figures.[97] Attempting to deny the Kremlin any possible change at influencing public opinion, the Ukrainian government attempted to generate a greater sense of national pride, which would spark greater commitment to a whole-of-society defense strategy.

The decentralization of Ukrainian society spread into a decentralized environment of civil-military cooperation. As the Ukrainian government struggled to supply Ukrainians fighting in the Donbas with resources, volunteers took it upon themselves to help supply Ukrainian fighters. Private military crowdfunding organizations arose starting in 2014. They all focused on providing well-tailored solutions to various problems. Most well known is People's Project which allows donors to choose from a variety of projects to help bolster Ukrainian military and volunteer capabilities. Come Back Alive and the Serhiy Prytula Charity Foundation focus on supplying infantry equipment, like body armor, ammunition, and communications devices. Army SOS, Drones for Ukraine Fund, and Aerorovidka work on drone development and procurement while the Ukrainian Cyber Alliance and the Cyber Partisans focus on cyberwarfare against separatist and Russian forces. These private charities expanded opportunities for participation both on the donation side as well as the procurement of goods to give to Ukrainian fighters. The volunteers charities also began contributing to the innovation and delivery of new technologies to the front lines by developing their own drones. As an alternative to the incredibly expensive foreign-made drones, the volunteers created their own drones in 2014, beating Ukroboronprom who only did so in 2016.[98] The charities rapidly adapted the drones and turned to commercial and hobbyist drones

[97] Paul A Goble, "Last Lenin Statue in Ukraine Falls - Euromaidan Press," Euromaidan Press, January 31, 2021, https://euromaidanpress.com/2021/01/31/last-lenin-statue-in-ukraine-falls/.
[98] Alshamy et al., "Polycentric Defense, Ukraine Style," 47.

to provide fighters with cost-effective capabilities. This represented civil society taking initiative to participate in national defense through finding asymmetric strategies to adapt EDT. The stresses of war and incapacity of the defense institutions led to the birth of a unique, Ukrainian model of defense innovation that broke the boundaries between closed military bodies and open civil society.

By 2021, Ukraine had fully committed its ROC into a comprehensive whole-of-society strategy legally grounding its total defense culture in doctrine and law. The 2021 Military Security Strategy titled "Military Security – Comprehensive Defense" announced the full transition and embrace of a comprehensive approach to national defense. It stated a clear aim of turning Ukraine's defense system and society into a "smart viable deterrence strategy" instead of "a weak country's response to a superior power."[99] The 2021 security strategy introduced a "National Resilience Concept" which outlined specific areas to strengthen resilience. It was further supported by the passing of the Law of Ukraine "On the Fundamentals of National Resistance" in 2021 that added a legal perspective to the total defense system.[100] Thus, as Shelest noted, Ukraine "demonstrates the interconnection and interdependence of the notions of defense and resilience for responding to asymmetric threats, or when outnumbered by an adversary", and teaches other states "the process of building national resilience should run parallel to building national defense."[101] These reforms embedded the values of adaptability, self-organization, and civil-military cooperation derived from smartness into Ukraine's defense architecture. It fused technological innovation with societal participation. In the context of the 2022 full-scale invasion, Ukraine this smart, bottom-up

[99] Volodymyr Zelenskyy, "Decree of the President of Ukraine No.121/2021," Preside of Ukraine, 2021, https://www.president.gov.ua/documents/1212021-37661.
[100] Verkhovna Rada, "Law of Ukraine on the Basis of National Resistance," Verkhovna Rada, 2021, https://zakon.rada.gov.ua/laws/show/1702-20#Text.
[101] Hanna Shelest, "Defend. Resist. Repeat: Ukraine's Lessons for European Defence," European Council on Foreign Relations, November 9, 2022, https://ecfr.eu/publication/defend-resist-repeat-ukraines-lessons-for-european-defence/.

framework had been slowly built since 2014. Over the course of eight years, Ukraine knit a fabric of state, society, and technology that turned smallness into collective strength and resilience.

Smartness and Resilience Flourish: The 2022 Russian Full-Scale Invasion of Ukraine

The 2022 Russian full-scale invasion of Ukraine has put Ukraine's whole-of-society approach to defense and its technological innovation ecosystem into overdrive. The ROC concept from 2014, based on total defense, was propelled forward with an emphasis on how smart, cost-effective technology could increase Ukraine's asymmetric advantages against Russia to surprise the enemy and ensure the survival of Ukraine. Decentralization and digitalization were clearly shown not to have been mere conveniences. Instead, they were lifelines which had served to form the fabric of Ukrainian society and allowed the nation to resist the Russian invasion. This fabric is one based on total national defense that requires all parts of society to innovate and adapt to ensure. Ukraine is producing new technology and mechanisms to innovate at an all-time speed. Ukrainian society is also being driven closer together as it unites behind the joint aim of defending Ukraine's survival.

This flourishing of smartness has been enabled by the transformation of the Ukrainian defense sector. Attempts were made during the 2014 to 2022 period to rid the Ukrainian defense apparatus of its Soviet-era platforms; however, a lack of government investment in R&D, bureaucratic procedures wrapped in red tape, and unclear funding avenues prevented many attempts at reform from producing tangible change. The invasion of Ukraine in 2022 marked a radical departure from previous practices and frameworks. The urgency of war created an innovate or die mentality in both the public and private sectors. Showing operational flexibility, Ukroboronporm was dissolved to rid Ukraine of its Soviet, restrictive baggage and transformed into a joint stock company called the Ukrainian Defense Industry (UDI). This innovative switch saw immediate success as UDI saw

a 69% year-on-year increase in arms sales to $2.2 billion between 2022 and 2023.[102]The government also made major changes in the Military Equipment and Weaponry (MEW) requirements to rapidly get rid of red tape.[103] First, the development process overseen by Ukroboronprom was vastly outsourced to the private sector, civil society organizations, and other non-traditional actors. Second, the adoption, service, and acquisition processes were reformed through regulatory changes that cut complex, time-consuming bureaucratic hurdles.

These reforms were met by a unified society ready through years of reform and eager out of national pride to defend the survival of their nation. In the first 2 days after the invasion began, 40,000 citizens joined the Territorial Defense Forces.[104] Civilians helped construct military defenses, made Molotov cocktails, and distributed food. Ukraine also made a IT army entirely made up of volunteer hackers and IT specialists to do everything they can to make the enemy feel uncomfortable with their actions in cyberspace and in Ukrainian land.[105] This unit has managed to leak data and shut down the websites of the Kremlin, Russian state-owned Sberbank, or Radio Belarus.[106] The previously mentioned private volunteer charities also went into overdrive crowdfunding resources to help frontline soldiers.

---

[102] Stocholm International Peace Reseach Institute, "The SIPRI Top 100 Arms-Producing and Military Services Companies in the World, 2023," SIPRI, 2023, https://www.sipri.org/visualizations/2024/sipri-top-100-arms-producing-and-military-services-companies-world-2023.
[103] Kateryna Bondar, "How Ukraine Rebuilt Its Military Acquisition System around Commercial Technology," Center for International Strategic Studies, January 13, 2025, https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.
[104] Scott Jasper, "Resilience against Hybrid Threats: Empowered by Emerging Technologies: A Study Based on Russian Invasion of Ukraine," in *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies*, ed. Panos M. Pardalos and My T. Thai (Springer International Publishing, 2023), 209–26, https://doi.org/10.1007/978-3-031-39542-0_10, 222.
[105] Daryana Antoniuk, "How Ukraine's Volunteer Hackers Have Created a 'Coordinated Machine' around Low-Level Attacks," The Record (Recorded Future, May 4, 2024), https://therecord.media/ukraine-volunteer-it-army-machine-low-level-attacks.
[106] Bill Toulas, "Ukraine Says Its 'IT Army' Has Taken down Key Russian Sites," BleepingComputer, February 28, 2022, https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/.

Given that a great portion of Ukraine's defense industrial base is located in eastern Ukraine, the country had to find rapid solutions to increase defense production in undamaged, non-Russian-controlled land. In the first two years of combat, Ukraine's biggest arms producers suffered major losses. Engine manufacturer Motor Sich and aircraft producer Antonov claimed a combined $601 million worth of damage to industrial assets.[107] As a result, Ukraine had to find alternative solutions to defense production. On the one hand, Ukraine simply increased government spending to the military, spending 20 times the 2021 level on arms and dual-use goods by 2023 reaching $30.8 billion.[108] While a substantial amount of the budget increase went to procuring foreign weapons, Ukrainian arms producers restored their facilities and increased production. Crucial to this domestic revival, Ukraine received foreign assistance from the U.S., EU, and NATO through military aid, training, and intelligence. Even with external support, the determination to rebuild domestic defense production and innovate has become a defining feature of Ukraine's smartness and resilience. As a testament to the resilience of these companies, 500 arms producers , which employ 300,000 people altogether, were said to be operational in Ukraine in 2024.[109] On the other hand, private companies and civil society have stepped up to meet the needs of Ukrainian defense.

Ukrainian society has expanded the range of military hardware, introducing new technologies at a scale that was unthought of. The private charities that began crowdfunding and developing technology in 2014 have only increased the scale of their operations. Other civilian based

[107] Kyiv School of Economics, "Report on Damages to Infrastructure from the Destruction Caused by Russia's Military Aggression against Ukraine as of January 2024," April 2024, https://kse.ua/wp-content/uploads/2024/05/Eng_01.01.24_Damages_Report.pdf, 29.
[108] Volodymyr Vlasiuk, Luke Cooper, and Brian Milakovsky, "A State-Led War Economy in an Open Market Investigating State-Market Relations in Ukraine 2021-2023," *LSE Conflict and Civicness Research Group*, June 4, 2024, https://peacerep.org/wp-content/uploads/2024/06/A-state-led-war-economy-in-an-open-market-DIGITAL.pdf, 19.
[109] Kateryna Kuzmuk and Lorenzo Scarazzato, "The Transformation of Ukraine's Arms Industry amid War with Russia," SIPRI, February 21, 2025, https://www.sipri.org/commentary/topical-backgrounder/2025/transformation-ukraines-arms-industry-amid-war-russia.

organizations have contributed like nongovernmental organization (NGO) Aerorovidka which is attaching captured and donated legacy anti-tank grenades and munitions to homemade drones, to attack Russian vehicles at a fraction of the cost of advanced drone and missile alternatives that may cost hundreds of thousands of dollars.[110] Aerorovidka's Delta system represents the "seamless integration of public and private digital capabilities" that increase Ukrainian resilience.[111] Delta is the result of persistent pressure from civil society to represent the interests of troops on the ground and not overarching defense establishment. Delta has played vital role in the defense of Kyiv, the counter-offensives in Kharkiv and Kherson, and the sinking of the Moskva ship.[112] With the recent implementation of AI, the system creates insights for fighter by overlaying data onto geospatial imagery with videos, maps, and intelligence reporting.[113] Thus, technologically literate citizens have contributed to the war effort by combining simple, multi-purpose disruptive technologies right from commercial shelves to counter the Russian army in a smarter and cheaper way.

The Ukrainian government further propelled societal participation through the announcement of the Brave1 platform. Launched in the spring of 2023, Brave1 has decentralized the procurement, testing, and adoption cycle. It taps into Ukraine's pre-existing digital infrastructure and culture to create a fast track to foster private-public partnerships by bypassing the traditional requirement cycles and formal requests to approve new technology. It connects start-ups, engineers and military units to fuse the civil and military domains, accelerate innovation, and provide real-time feedback

[110] hDavid Hambling, "Only the Brave: How Ukrainians Can Take on Russian Tanks with Molotov Cocktails," Forbes, March 2, 2022, https://www.forbes.com/sites/davidhambling/2022/03/02/only-the-brave-how-ukrainians-can-take-on-tanks-with-molotov-cocktails/.
[111] Audrey Kurth Cronin, "Open Source Technology and Public-Private Innovation Are the Key to Ukraine's Strategic Resilience," War on the Rocks, August 25, 2023, https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience/.
[112]Mykhaylo Lopatin, "Bind Ukraine's Military-Technology Revolution to Rapid Capability Development," War on the Rocks, January 23, 2024, https://warontherocks.com/2024/01/bind-ukraines-military-technology-revolution-to-rapid-capability-development/.
[113] Cronin, "Open Source Technology".

between front-line forces and developers. In just a few months after its release, Brave1 registered approximately 400 projects focused on drones, robotic systems, electronic warfare, artificial intelligence tools, cybersecurity, communications, and information security management systems.[114] Since then, it has grown to support over 1,500 military technology start-ups.[115] Brave1 has enabled the development of technology that makes up core elements of the EDT landscape. It represents one of the world's most decentralized EDT incubators, accelerating past bureaucratic barriers to bring grassroots technology into the hands of soldiers on the frontline.

Ukraine's drone industry has also exemplified the forces of decentralization, digitalization, and innovation all working together to increase Ukrainian resilience. Through its experience with drones and Russia's subsequent adaptations, Ukraine has come to learn that all advantages are temporary. As a result, the ability to adapt and scale innovations the quickest is more important than a specific technology. As a result, a whole-of-society strategy is required to make sure all functions of the state and society are working in unison to innovate, implement, and defend.

Under the conditions of war, Ukraine's digitalization clearly appears as a meticulously built, intentional network meant to bolster the country's resilience. The digital network of Ukraine has been built to address the needs of citizens as efficiently and quickly as possible. Its services allow for life to continue for citizens with all the daily necessary functions as basic as internet connection. While credit must be given to international aid like the establishment of Starlink terminals throughout Ukraine, Ukraine did not digitalize overnight. It was a process that evolved over the past 11 years. To have digital services standing and thriving despite being under constant

[114] Mykhailo Fedorov, "Ukraine's Vibrant Tech Ecosystem Is a Secret Weapon in the War with Russia," Atlantic Council, August 17, 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-vibrant-tech-ecosystem-is-a-secret-weapon-in-the-war-with-russia/.
[115] Kuzmuk and Scarazzato, "The Transformation of Ukraine's Arms Industry.

attack sends a blaring message to the rest of the world: Ukraine is functioning, innovating, and thriving at full force.

Since the start of the war, the Diia app has been expanded to deal with war time realities. War bonds can easily be purchased to support the war economy, citizens can report enemy troop movements, national media and television can be streamed, and documents are centralized in one place allowing for easy movement between checkpoints. With 12 million people who have been displaced by the conflict, the Diia app has been instrumental in keeping track of Ukrainians who have been forced to move abroad. An Internally Displaced Person (IDP) status portal was created to support the person while abroad by allowing them to establish their identity without physical documents. This ability to track displaced Ukrainians will also be incredibly helpful for Ukraine to welcome back the displaced post-war. This IDP integration has also led to neighboring countries to accept Diia, spreading the influence of Ukraine's digitalization reforms to European neighbors. Diia has also been used as a financial aid platform for Ukrainians to request funds to help cope with the destruction of their homes and communities. Diia has incorporated various types of EDT, adding facial recognition to verify IDP registration and AI-assisted damage assessments.

Additionally, this digitalization has increased Ukraine's intelligence, surveillance, and reconnaissance (ISR) capabilities, further strengthening Ukraine's resilience. Through apps like Diia, Telegram, and Viber, Ukrainian citizens can upload geotagged images, videos, recordings, and messages of updates concerning the movement of Russian forces to chatbots. This innovation has transformed phones into data-collection devices. In the first month of the war alone, 260,000 individuals used the Diia app to report Russian activity.[116] By using AI algorithms to create

[116] Yaroslav Druziuk, "A Citizen-like Chatbot Allows Ukrainians to Report to the Government When They Spot Russian Troops — Here's How It Works," Business Insider, April 18, 2022, https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4.

chatbots like the eVorog bot on Diia and the @stop_russian_war_bot on Telegram, thousands of civilian reports are turned into intelligence datasets.[117] This has been especially effective for gaining intelligence, surveillance, and reconnaissance (ISR) about Russian-controlled territories in Ukraine. At the same time, websites like Live Universal Awareness Map use open-source intelligence to gather information from media sources to create a map of Russian movement across Ukraine, updated in real time, with signals for the type of activity being reported. By taking advantage of technological interconnectivity and the national responsibility to defend the state from Ukraine's total defense concept, all of Ukraine has been transformed into a system of sensors that constantly communicate to ensure the survival of the Ukrainian state and people.

What Does This Mean for Ukrainian Resilience?

Defying all expectations of how a small power can resist the military attack of a greater power, Ukraine has demonstrated the power of resilience. Its slow build of a total defense approach which built a national culture of contributing to defense shows that resilience does not grow over night. What makes Ukrainian resilience unique is its organic, bottom-up, decentralized nature. This approach spreads across the government's approach to individual Ukrainian volunteers, civil society groups, and private sector actors. Across all sides of Ukrainian society, resilience has been grounded in a unified, collective spirit of adaptability, self-organization, and civil military fusion. While Ukraine only formally committed to total defense in 2021, it had set a foundation in the years following 2014. In the face of existential threats, the decentralized and digital channels have created an ecosystem of innovation in Ukraine has thrived outside traditional channels. This

[117] Robin Fontes and Jorrit Kamminga, "Ukraine a Living Lab for AI Warfare," National Defense, March 24, 2023, https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.

unconventional approach only adds to Ukraine's smartness, engages more of Ukrainian society, and strengthens resilience

The Ukrainian case had revealed that it is not EDT which in isolation increases resilience. Instead, this study of Ukraine suggests that it is the Total Defense concept which has technological innovation deeply embedded into it. In Ukraine's case, resilience stemmed from a nation-wide spirit where innovation is not confined to just the state or just the private sector but distributed across the entire society. This innovation is empowered through various platforms, networks and initiatives which the state nurtured. That stead EDT still plays a vital role in the resilience of Ukraine. As the war continues, Ukraine is being demographically depleted and EDT like unmanned vehicles can help account for this loss in life and keep more Ukrainians away from direct military confrontations.

While technology is essential to conflict, as Clausewitz posits, war is not purely a technological or military endeavor. War depends on humans and societies. Thus, through closer civil-military fusions, technology is allowing citizens to both see more war and participate more in war. Ukraine reveals that people enhance deterrence. Ukraine's survival is not just a matter of drones, missiles, and satellites. It is based on long term public indoctrination into a whole-of-society approach based on survival. At the point of existential crisis, Ukrainians have chosen *smartness*, producing a cheap, data-driven, adaptive battlefield network. While Ukraine's whole-of-society ethos may have been unable to deter a Russia invasion in 2022, the impact of this strategy may serve to deter future wars. Everyone, from soldiers to civilians to President Zelenskyy, are integrated into an interlinked society fighting to strengthen the nation.

Chapter V: Estonia

Introduction

This case study will explore the story of Estonia's development following the collapse of the Soviet Union in 1991 until the present day. Since its independence, Estonia and its leadership have decided to pursue aggressive policy reform and establish itself as a hub for innovation. Estonian leadership prides itself on cultivating a national culture that takes initiative, embraces risk-taking, and is entrepreneurial. Estonia bore its smartness through its radical digitalization initiatives, which were unheard of for their time. Developing the model of e-Estonia, Estonia wove every fiber of society together through cyber platforms that further encouraged participation in society. These innovation-forward policies were supported by a constant effort to build national pride and unity. Beginning with national conscription and training exercises, Estonia has established a comprehensive, whole-of-society approach to defense that uses every resource to defend the country. Accelerated by the 2007 cyberattacks, this comprehensive defense has made Estonia more digitally interconnected and innovative and, in that process, more resilient.

What Makes Estonia Small?

As the smallest of the three Baltic states, with a total area of 45,227 square kilometers and a population of around 1.3 million, Estonia exemplifies the classic case of a small power in both absolute and relative terms. Throughout its history, Estonia has been shaped by its attempts to exert regional power over its surrounding neighbors, having lost its independence due to Soviet invasion during the mid-20th Century and facing renewed threats from Russia. Estonia's smallness, however, has not meant passivity. Instead, Estonia has embraced its limitations and committed to turning them into advantages, shaping its defense forces into a compact force, implementing

military conscription, and deploying unconventional strategies instead of direct power projection. Rather than trying to match adversaries head-to-head, Estonia has simultaneously pursued security independence while also using economic and defense integration into Western institutions like the EU and NATO. Though Estonia does not get much respite from its geography, lacking strategic depth and vulnerable to threats from the Baltic Sea, Estonia has leveraged smart diplomacy, advanced technological innovation, and comprehensive societal resilience to overcome the constraints of its smallness.

Starting with Smartness

Soviet Shambles to Societal Strength

Prior to the collapse of the Soviet Union, Estonia had been independent multiple times. First, in 1918, Estonia became independent shortly after the end of World War I (WWI) and the establishment of the League of Nations. Estonia became politically isolated; however, as the League of Nations weakened, the Soviet Union and Germany became more aggressive, and the rest of Europe erred on the side of avoiding the risk of war. As a result, Estonia declared political neutrality in 1938, but the declaration was meaningless since Estonia lacked the military capacity to defend its neutrality. By 1940, Estonia's first try at independence ended with Moscow annexing the country. Subsequently, Estonia was engulfed into the Soviet Union until 1991 when the union dissolved.

Upon its independence in 1991, Estonia had bleak prospects. 50 years of communist rule left Estonia with a food shortage, no currency, depleted production capabilities, and no pre-existing economic ties. Inflation was at 1,000% and the population of Tallinn, Estonia's capital, had moved

to the countryside to cope with food scarcity.[118]Additionally, Estonia lacked private business, the food market crumbled without its top-down state control, money had no value, and savings were worthless. Estonians had no drive or motivation as life under the Soviet Union had repeatedly created unproductive job security. Estonia had non-existent military capabilities, lacked human resources, no legal or conceptual framework for national defense, and few financial resources to build security.

In order to deal with this dire situation, its first leaders committed to rapid reform. After becoming independent, Estonia's leaders, specifically Mart Laar who served as Prime Minister from 1992-1994 and 1999-2002, proclaimed that Estonia would be known for trying new policies and labelled Estonia as an innovation hub. Applying shock therapy, Laar and his cabinet focused first on economic development. Estonia implemented price liberalization, introduced its own currency called the kroon, and deployed a tight fiscal policy. Additionally, Estonia privatized all industries and opened the country foreign direct investment. Leadership flipped Estonia from a centrally planned economy to a free trade center. Laar pushed for a balanced budget, which was painful at first but eventually became Estonia's brand and source of constant economic surplus.

In order for Estonia's rapid reform to succeed, Laar understood that he needed to regain public trust. Laar needed to gain political consensus and legitimacy to allow for rapid reform. Without national support for innovative, risky policies, national divide might have spread, denying Laar any chance to implement extraordinary, alternative, unconventional solutions. Laar faced the additional hurdle of a demographically diverse population. To this day, Estonia remains diverse. The nation's ethnic breakdown is currently 69% Estonian, 25% Russian, 2% Ukrainian, 1%

[118] Armen Sarkissian, *The Small States Club: How Small States Can Save the World* (London: C. Hurst & Co., 2024), 114

Belarusian, 0.8% Finnish, and 1.6% other.[119] Thus, Estonian leadership prioritized democracy through consensus-based decision making, accountable institutions, and free and fair elections. By presenting Estonians with a democratic choice, Laar and his cabinet grew bottom-up demand that welcomed his top-down proposals.[120] This bottom-up approach also unified Estonians on equal footing regardless of their ethnic background.

Additionally, the government revitalized the nation by enabling entrepreneurship and growth. The state reversed the Soviet past of state control and decay by stressing that Estonia would only help those willing to help themselves.[121] While the policy was unpopular at first, the state committed to the strategy and doubled down, encouraging economic individualism, initiative, and risk taking. These policies increased participation in economic activities by citizens and grew competition. Simultaneously, Laar relinquished regulatory control and eliminated subsidies and selective privileges to eradicate sources of corruption. Companies that received government funding before had to adapt and innovate to survive or risk collapsing under bankruptcy.

Estonia also implemented a unique tax system that contributed to the general spirit of innovation which had grown to define the country. By implementing a flat tax, the state made tax collection a simple, streamlined process that was easier for taxpayers and fiscal officials. A flat tax shed excessive paperwork and complex calculations, so officials could crack down on tax evasion. A direct rejection of the traditional European tax collection method, a flat tax improved efficiency, increased tax law compliance, and eliminated the shadow economy lingering from Soviet rule. Additionally, Estonia's tax system further fueled entrepreneurship. Income reinvested in enterprise development was declared exempt from taxes. Personal income tax matched the corporate tax rate

[119] Central Intelligence Agency, "Ethnic Groups - the World Factbook: Estonia," CIA, December 23, 2021, https://www.cia.gov/the-world-factbook/about/archives/2021/countries/estonia.
[120] Sarkissian, *The Small States Club*, 117.
[121] Ibid.

of 20 per cent and did not apply to dividends. As well, property tax was imposed only on land, excluding real estate and capital. Due to these policies, Estonia grew as a hotbed for entrepreneurs. While in 1992, Estonia had around 2,000 registered businesses, by 1994 the number jumped to 70,000.[122] To this day, Estonia has the most startups per capita in Europe with €1,967 per capita raised and one startup per 1,048 people.[123] Despite having reformed Estonia's economy and having started to gain public trust, Estonia remained defenseless against potential adversaries.

When Estonia gained independence in 1991, it saw itself as having three possible security options. First, Estonia could pursue neutrality like it had in the early 20th Century and like Finland had managed. Second, Estonia could establish strong relations with post-Soviet states from the Commonwealth of Independent States (CIS), specifically Russia. Finally, Estonia could integrate into the Western economic and security structure. Not declared until 1996, the official defense policy released by the Estonian Parliament, or *Riigikogu*, declared that the "Guidelines for the Estonian National Defense Policy," would be based on two foundations: independent self-defense capability and international defense-related cooperation.[124] Estonia set its defensive goal as survival and sovereignty.

Estonia's approach to defense was based on three militaristic experiences. First, prior to WWII, Estonia experienced war and gained a strategic self-evaluation. In their fight for independence from the Soviet Union, Estonians learned their geography and developed a national fighting strategy. At the time, Estonia faced its most existential threat. In an attempt to fight for survival, Estonian forces crossed the forest-dominated terrain of the country and developed a forest

[122] Sarkissian, *The Small States Club*, 120.
[123] Invest Estonia, "Estonia Leads Europe in Startups, Unicorns and Investments per Capita," Invest in Estonia, December 2022, https://investinestonia.com/estonia-leads-europe-in-startups-unicorns-and-investments-per-capita/.
[124] Riina Kaljurand, "Security Challenges of a Small State: The Case of Estonia," in *Defense and Security for the Small: Perspectives from the Baltic States*, 2013, 63.

warfare style which Estonia has since perfected. The next experience was the post-Soviet Estonian soldiers who had fought on behalf of the USSR prior to 1991. Serving in the Afghan-Soviet war, these soldiers learned the Soviet fighting style. Upon returning from the war and soon becoming independent, the soldiers combined this new fighting style with their Estonian style to define the new Estonian military apparatus. Finally, Estonia's accession to NATO in 2004 served as another defining evolution. Joining NATO added a layer of security through NATO's guarantee of collective action. Additionally, Estonian military forces learned modern Western tactics from other countries through joint training exercises. Estonia, however, did not join NATO in order to hand off the job of security to its bigger, more powerful allies. For Estonia, as a military expert from the Estonian Defense Forces anonymously claimed, "NATO is not the aim, [it is] a mean."[125] Unlike other NATO members, Estonia has not relied on the alliance for military protection. Estonia has remained wary of the ambiguity that surrounds the untested Article 5 provision and collective defense. As a result, Estonia has kept mandatory military conscription, unlike its Baltic counterparts, Latvia and Lithuania. Additionally, Estonia has never stopped training its soldiers in its national fighting style.

While Estonia has developed its security and defense model in close relation to NATO, the country has fought to maintain the ability to work independently to ensure maximum security in time of crisis. In order to do so, Estonia has embraced its smallness and attempted to maximize its smartness. Estonia's smallness, combined with its passionate political campaigns toward rebuilding the country, have worked positively to shape its nascent military model. Through this strategy, Estonia has developed a system in which embracing the limitation if smallness creates a need to innovate in order to increase smartness. These two mutually reinforcing attitudes feed back

[125] Irina Ispas, "Principle of Military Innovation as an Upgrade to the Army Concept: Differences, Similarities and Lessons. A Case Study of Israel and Estonia." (2019), 26.

into each to create a model where the entirety of Estonian society collaborates in unison to back the state's survival with a comprehensive total defense strategy.

Decisive Digitalization

Estonia did not accidentally stumble upon technology and digitalization as a solution to its smallness. Digital innovation was a national survival strategy that was deliberately chosen both because of its innovative, daring nature for its time and solution to overcome Estonia's resource constraints. The leaders of Estonia understood their position of limited resources and embraced a domain where scale and smartness could compensate for smallness– the digital sphere.

Estonia's digital development is defined by the nation's alternative title: e-Estonia. e-Estonia is the nation's most ambitious undertaking, which has come to define the identity of every facet of society. e-Estonia takes its roots from Soviet times when Estonia was the epicenter of technological advancement and software development as well as at the forefront of education policy.[126] e-Estonia's origins began in the education and banking sectors. Launched in 1996 by the then Ambassador to the United States and future President of Estonia Toomas Hendrik Ilves, then Minister of Education Jaak Aaviskoo, and then President of Estonia Lennart Meri, the Tiger Leap Initiative was an attempt to modernize the education system by expanding access to computer infrastructure.[127] The results of the program were almost immediate as 97% of Estonian schools had access to the internet within the program's first year.[128] By equipping schools with computers and internet, Estonia molded its future generations into a digitally literate generation that valued

[126] Joseph M. Ellis, "Estonia's Innovation Culture: How Did It Happen?," Foreign Policy Research Institute, December 7, 2016, https://www.fpri.org/article/2016/12/estonias-innovation-culture-happen/.
[127] Education Estonia, "How It All Began? From Tiger Leap to Digital Society," Education Estonia, n.d., https://www.educationestonia.org/tiger-leap/.
[128] Owain Llŷr Talfryn, "Learning from Estonia: How a Young Nation Became a Leader in Digital Living.," Stellar Capacity, December 23, 2021, https://www.stellarcapacity.com/post/learning-from-estonia-how-a-young-nation-became-a-leader-in-digital-living.

technology. Stemming from Mart Laar's desire to digitize and automate privatized banking systems, Estonian banks introduced national electronic banking in 1996 as well to ensure simple, transparent, and secure transactions.[129] Additionally, banks partnered with telecommunications companies to offer free courses on computing and how to use smart devices safely. The digital banking initiative serves as an early example of digital, smart strategies coming not just from forced government policy but voluntary buy-in from the private and civilian spheres

This e-Estonia model prompted the birth of Estonia's e-government through the Estonian parliament's announcement of its Estonian Information Policy Principles in 1998. The principles aimed to empower citizens through digital services in order to facilitate economic transition and development. It structured the e-government model to prioritize eliminating unnecessary and time consuming systems, empower citizens by allowing them to carry out procedures through quick means, and minimize bureaucracy through digital tools that could authenticate actions faster. The Estonian leadership believed that digitalization would remove barriers to entrepreneurship and capital accumulation leading to economic growth and development. This process would increase confidence in government policy creating a feedback loop where public consensus would foster innovation.

The e-government model was based on the pillars of the "X-Road" platform and electronic national identification (e-ID). Introduced in 2001, "X-Road" is a system built to send and receive data between the public and private sectors. It allows for stable, secure interoperability between the state and businesses where data can be passed quickly. Its success manifests itself in its usership with more than 2,300 public and private services depending on the platform.[130] It is estimated that

[129] Victor I Espinosa and Antonia Pino, "E-Government as a Development Strategy: The Case of Estonia," *International Journal of Public Administration* 48, no. 2 (February 16, 2024): 1–14, https://doi.org/10.1080/01900692.2024.2316128.
[130] Sarkissian, *The Small States Club*,121.

the system saves the Estonian government nearly 2% of GDP and 800 working hours annually.[131] The success of "X-Road" has been so profound that its open-source code was published in 2016 by MIT and integrated into Finland's data exchange system starting in 2018.[132] In 2002, Estonia introduced a mandatory electronic identification card and digital ID pin. This e-ID is every citizen's key to the full range of e-services in Estonia ranging from e-taxes to parking to public transport. In 2005, Estonia announced i-Voting transitioning nationwide voting onto the internet and computers in order to increase government participation.[133] i-Voting made Estonia the first state in the world to implement remote voting through electronics. In 2011, Estonia expanded electronic i-Voting to enable voting by mobile text message.[134]

The effects of Estonia's innovative digitalization spread through the roots of Estonian society. Digitalization created a foundational layer from which Estonia produced a whole-of-society approach based on technological innovation. Estonians were proud to be one of the most innovative countries in the world. Thus, the private sector responded to the public sector reforms.

Turning Smartness into Defense: The 2007 Cyberattacks

The 2007 Russian cyberattacks revealed to Estonia that defense was more than just rifles and soldiers but a project that required comprehensive, total societal participation. In 2007, Estonia faced one of the first cyberattacks against an entire nation ever recorded.[135] Built in 1947, the Bronze Soldier Statue was built to commemorate the Soviet soldiers who died during WWII while capturing Tallinn. In the spring of 2007, the Estonian government decided to move the monument

[131] Ibid.
[132] Ibid.
[133] Espinosa and Pino, "E-Government as a Development Strategy".
[134] Ellis, "Estonia's Innovation Culture".
[135] Joel Burke, "Inside Estonia: How the EU's E-State Thinks about Defense Tech," *Emerging Technologies Institute*, September 2024, 1–9, 4.

dedicated to Soviet troops away from an intersection in the center of Tallinn to a cemetery on the outskirts of Tallinn because the statue had taken on two very different, polemic identities. For the Russian minority in Estonia the Bronze Soldier represented the USSR's victory over Nazism, hence the statue's name "Monument to the Liberators of Tallinn." For Estonians, however, the statue represented the oppression that the Soviet Union had forced onto Estonia for half a century. In an attempt to diffuse tensions between pro-Kremlin and Estonian nationalist movements, the Estonian government decided to move the statue beginning on April 26, 2007. While peaceful protests gathered throughout the day, by night protests became violent resulting in clashes with the police. Over the course of two nights of protests, 156 people were injured, one person died and 1,000 people were detained.[136] At the same time, Estonia faced its first cyber-attack on April 27 against its internet-facing systems, leading to a 22-day period of attacks.[137] While the types of cyberattacks were known, the scale and variety which were unleashed on Estonia were unparalleled. Estonia's public digital services were paralyzed as Estonia's bank, media, and government websites were flooded with spam and automated online requests. In addition to the protests in Tallinn and cyberattacks against Estonia, pro-Kremlin youth groups protested outside the Estonian embassy for multiple days, preventing the embassy workers and diplomats from leaving or entering the building. The climax occurred on May 2, 2007, when an Estonian ambassador was physically attacked during a press conference.[138] Thus, the 2007 cyberattacks momentarily crippled Estonia. Cash machines and banking services disappeared, government

[136] Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News*, April 27, 2017, https://www.bbc.com/news/39655415.
[137] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *NATO Cooperative Cyber Defence Centre of Excellence*, 2008.
[138] Ibid.

employees could not communicate with each other, media sources could not deliver news, local enforcement could not peacefully tame protests, and Estonians abroad were under threat.

The 2007 protests and cyberattacks can be seen as a turning point in Estonian history from which point forward Estonia took full force of its smartness to defend the state and bind Estonian society behind a mission of national security. Given that the attacks targeted the lifelines of Estonia, digital services, Estonia realized that it needed to gather all of society behind the unified goal of bolstering all aspects of its security. The attacks were not a mere threat to digital services, but to the entire national security of the state. It represented an existential attack on Estonia. The novelty of cyberattacks revealed that Estonia was not just facing the threat of kinetic attacks or military invasion. Its main adversary was waging full hybrid war, therefore all of society needed to be prepared in case of an attack both to be able to recover but also to be able to respond. The attacks proved that country despite having a developed network of infrastructure was susceptible to these attacks and other forms of hybrid war. Thus, it was beyond a question of having proper, indestructible infrastructure. Society and people needed to be resilient as well.

While Estonia's security and defense policy has embraced a small, smart strategy since Estonia's independence in 1991, the 2007 Russian cyberattacks against Estonia propelled Estonia to fully embrace a comprehensive whole-of-society approach to defense. The shock of the attacks revealed that damage of cyberattacks was not just reserved to individuals or singular organizations but could cripple the functioning of an entire state, paralyzing the public and private sectors in addition to the general population.

The concept of total defense, or *totaalkaitse*, had existed as a concept in Estonia since its independence. Throughout the 1990s, total defense was understood as the usage of all available resources towards state defense. This progressed to the 2001 Military Defense Strategy, which

defined total defense as "the permanent psychological, physical, economic and other types of readiness of the state and municipal institutions, defense forces and the whole society to manage crises."[139] A problem with this original definition is that it allows for society to hide behind its military and support its country's defense passive sense. Given the size of small powers and the reality of hybrid warfare today that attacks all facets of society, this definition of total defense was inadequate. Thus, the concept of a comprehensive approach, or *kõikkehõlmav lähenemine*, was introduced in 2004, greatly influenced by Estonia's accession into NATO in the same year.[140] Under this new framework, Estonia applied a policy based on resilience and deterrence.

2010 represents a monumental year in which Estonia fully embraced a comprehensive whole-of-society approach to defense. Replacing the National Military Strategy, the National Defense Strategy declared a switch in Estonia's security policy to focus "on a broad concept of security, entailing all trends affecting security and essential areas required for ensuring security."[141] It recognized the beginning of new, hybrid threats that were not confined to the kinetic realm which attacked the "cohesion of Estonian society" and required " cohesion of Estonian society necessitate greater attention to the sense of cohesion and psychological defense."[142] The National Defense Strategy put forward the six pillars of Estonian comprehensive defense: military defense, civilian support, international action, internal security, continuous operation of the state and society, and psychological defense.[143] The document also formally used the term "resilience" for the first

[139] Viljar Veebel et al., "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force," *Journal on Baltic Security* 6, no. 2 (December 8, 2020), https://doi.org/10.2478/jobs-2020-0007, 3.
[140] Veebel et al., "Territorial Defence, Comprehensive Defence," 3.
[141] Estonian Parliament (2010) *Eesti julgeolekupoliitika alused* [Estonian National Security Concept] https://www.riigiteataja.ee/aktilisa/0000/1331/4462/13316508.pdf
[142] Estonian Parliament , "Eesti Julgeolekupoliitika Alused [Estonian National Security Concept]," 2010, *https://www.riigiteataja.ee/aktilisa/0000/1331/4462/13316508.pdf*.
[143] Kaljurand, "Security Challenges of a Small State," 65.

time.[144] The word resilience does not have an Estonian equivalent, so the word *kerkus* was introduced.

While *kerkus* is used, the word *Siil* is thought to better represent the concept of resilience in Estonia. *Kerkus* was defined as society's ability to recover quickly from a shock.[145] *Siil* translates to hedgehog. The hedgehog serves as the symbol of Estonian defense. While little and hardly able to fully stop a Russian bear, a hedgehog can severely injure the bear with its spikes when it takes a defensive posture. For Estonia, these spikes, however, are not just made from the military but every part of Estonian society: its people, institutions, digital platforms, and a unified will to resist. Estonia acknowledges as well that comprehensive defense is not a one off process that has a beginning and an end. It is phased and constantly evolving in parallel to changes in defense and security priorities and evolving threats.

The 2017 National Defense Strategy saw an increased focus on the relationship between resilience and the cohesion of society. Unlike previous strategies, the 2017 framework lays the concepts of whole-of-government and whole-of-society as the foundation for merging the concepts of comprehensive defense and resilience. It reinforced the notion that Estonia's defense lies first at home with societal cohesion, decentralized readiness, and psychological rigor. The strategy also created an avenue for strategic continuity by introducing the 2017-2026 national defense development plan which reaffirmed the six pillars of comprehensive defense. Building on the 2017 strategy, Estonia recently released the National Defense Development Plan for 2022-2031

Notably, the invasion of Georgia in 2008 and events in 2014 in Ukraine did not spark major changes in the Estonian defense apparatus or development plans; instead, the events simply

[144] Tony Lawrence, "Estonia: Size Matters," *PRISM* 10, no. 2 (March 10, 2023): 19–37, 21.
[145] Piotr Szymański, *New Ideas for Total Defense: Comprehensive Security in Finland and Estonia* (Warsaw, Poland: Centre for Eastern Studies, 2020), 36.

confirmed Estonian convictions that Russia is an aggressive state willing to invade its neighbors.[146] In order to increase Estonian resilience, the government approved the Civil Protection Concept.[147] Creative tools were introduced to counter Russian influence while bolstering Estonian national identity like the creation of Estonian Russian language television and radio channels, blogs, and counter-disinformation websites. According to certain sources, Estonia's efforts to integrate the Russian-speaking population into Estonia have succeeded as 90% are integrated.[148]

The Estonian *Kaitseliit*, or Defense League, a non-political voluntary paramilitary organization, plays a major role in the comprehensive defense of Estonia and building national spirit. Under the Estonian Defense League Act, it has been integrated into the Estonian armed forces assigned to increase Estonian security by training Estonian citizens to improve their defense skills. The League has a core of nearly 16,000 volunteers and is organized into 15 battalions, so each country, or *malev*, of Estonia has a battalion.[149] The *Kaitseliit* accomplishes its goal of increasing security not just by literally training Estonians to fight but also by spreading patriotism and the understanding that all Estonians are responsible for fighting on behalf of their state. The Defense League has spread this spirit of civil-military cooperation through its various offshoots like the 'Women's Voluntary Defense Organization', the Girl-Scout-equivalent organization 'Home Daughters', and the scout-type patriotic youth paramilitary organization 'Young Eagles.'[150] Initiatives such as those led by the Estonian Defense League seem to pay off given the reported

---

[146] Andres Vosman and Magnus Petersson, *European Defence Planning and the Ukrainian Crisis: Two Contrasting Views*, Institut Français des Relations Internationales (IFRI), 2015.
[147] Republic of Estonia: Government Office, "The Government Approved a Comprehensive Approach towards Development Civil Protection," 2018, https://www.valitsus.ee/en/news/government-%20approved-comprehensive-approach-towards-developing-civil-protection.
[148] Paul Goble, "Experts: Estonia Has Successfully Integrated Nearly 90% of Its Ethnic Russians," Estonian World, March 1, 2018, https://estonianworld.com/security/experts-estonia-successfully-integrated-nearly-90-ethnic-russians/.
[149] Stephen J. Flanagan et al., "Deterring Russian Aggression in the Baltic States through Resilience and Resistance," *RAND Corporation*, April 15, 2019, 8
[150] Veebel et al., "Territorial Defence, Comprehensive Defence," 8.

81% of Estonians willing to participate in armed resistance in the event of an attack.[151] Thus, trust built between the civil and military sectors fuels Estonia's defense strategy and enables its whole-of-society strategy.

Through digitizing, Estonia has a system of communication between policy makers, government administrators, and private sector leaders that complements its comprehensive defense model. As Current Minister of Defense Hanno Pevkur stated that the title Comprehensive Defense or Total Defense is irrelevant. For Pevkur, the slogan "every bush shoots" best captures the "wide approach to defense" which Estonia has adopted where everyone has a role in defending the state as all facets of life are tied to the defense of the state.[152] Thus, Estonia's complex digital network and high emphasis on technological innovation have created a civil-military culture that aims to make "every bush shoot" through technological means. Building on the 2017 strategy, Estonia recently released the National Defense Development Plan for 2022-2031. This new plan directly confronts the reality of the deteriorating security environment in Europe since Russia's invasion of Ukraine. It emphasizes the need for the civil and military sectors to be interoperable, for infrastructure to remain resilient, and for regional cooperation with NATO, the EU, and other regional partners like Ukraine to deepen. The plan calls for deeper integration between the *Kaitseliit* private sector technology leaders, local civic leaders, and national services. The concept represents a shift in comprehensive defense as a theoretical concept to a concrete and implemented posture with its roots spread across all aspects of national life.

[151] Józef Witold Jordan, "Evolution of the Concept of Total Defence in the Baltic States," *Rozprawy Społeczne* 18, no. 1 (July 11, 2024): 315–44, https://doi.org/10.29316/rs/188761, 338.
[152] Hanno Pevkur, Interview with the Honorable Hanno Pevkur: Minister of Defense of Estonia, interview by Michael Miklaucic, *PRISM (National Defense University Press)*, June 2, 2023, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3512177/interview-with-the-honorable-hanno-pevkur-minister-of-defense-of-estonia/.

The technological lifeline of Estonia's comprehensive defense has relied on cyber and drone capabilities. Starting in 2008 after the cyberattacks, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) was established, reinforcing Estonia's position as a global leader in cybersecurity capabilities. One of the largest Centres of Excellence in NATO, the CCDCOE has cemented Estonia as the global hub of cyber. It produced the Tallinn Manual, laying the legal groundwork for confronting the legal and policy side of cyber issues. It also coordinated the 2023 Operation Locked Shields, which was the world's largest cyber exercise, connecting over 3,000 participants from 38 countries.[153] This type of global display of Estonia's innovative and resilient society serves as a defense tactic. It symbolizes Estonia's strategy of using technology to unify the military, civilian, and private sector to co-produce resilience. It allows Estonia to project itself as the "E-capital of Europe" and a leader in the cyber sphere.[154] By flexing its capabilities, Estonia signals the strength of its comprehensive approach.

Estonia's comprehensive approach is further strengthened by its structural reforms aimed at increasing public-private innovation to bolster defense. As High Commander of Estonian Defense Forces General Riho Terras stated in 2018, "[military] innovation is being carried forward by the Estonian society as a whole."[155] In 2017, Estonia created the Estonian Centre for Defence Investment to radically consolidate the nation's entire defense procurement functions.[156] On the supply side, the formation of the Estonian Defense Industry Association has created a singular node for the triple helix of Estonian society– industry, R&D organizations, and government– to

[153] NATO Cooperative Cyber Defence Centre of Excellence, "World's Largest Cyber Defense Exercise Locked Shields Brings Together over 3000 Participants," NATO CCDCOE, April 18, 2023, https://ccdcoe.org/news/2023/6016/.
[154] Ispas, "Principle of Military Innovation," 31.
[155] Ispas, "Principle of Military Innovation, 29.
[156] Tomas Jermalavičius and Martin Hurt, "Defence Innovation: New Models and Procurement Implications – the Estonian Case," *Armament Industry European Research Group, French Institute for International and Strategic Affairs (IRIS)*, September 2021, 1–23, 7.

unite and explore cooperation areas in EDT development specifically in AI, space, cyber, and unmanned autonomous vehicles.[157] This ecosystem empowers fast adaptation and feedback loops between users and producers to create state and socially embedded technology. CR14, established by the MOD in 2020, represents an unconventional strategy deployed by Estonia. CR14 is a cyber range where the Defense Forces Cyber Command, Cyber Defense Unit of the EDL and NATO CCDCOE partners can train and test deploying and defending against cyber capabilities.[158] Following in the spirit of Estonian *smartness*, Estonia is currently working on an Open Cyber Range for cyber innovators, ranging from startups to established companies to individuals, to conduct exercises and test new ideas and technologies.

Estonian startups have thrived at the intersection of civilian and military needs. With the announcement of the €100M Defense Industry Fund managed by SmarCap, Estonia has promised to focus investments on EDT through AI, drone, and cybersecurity start-ups. While Cybernetica is considered to be the "grandfather of Estonia's cybersecurity sector," Veriff, CybExer, and RangeForce are all emerging cyber leaders established in the mid-2010s.[159] Given the small, collaborative nature of Estonia, these companies have all evolved from past cyber competencies. Outside of cyberspace, Milrem Robotics, Threod Systems, and Desecintl all present successful stories. Milrem Robotics is a leader in unmanned ground vehicles, supplying 18 countries, including Ukraine, with their AI-powered THeMIS and Type X drones.[160] Threod Systems, established in 2012, creates unmanned aerial systems (UAS) designed for ISR capabilities. Used by the UAF and at least 24 other countries, all of Threod's products are made in-house in order to

[157] Ibid, 8-9.
[158] Ibid, 9.
[159] Burke, "Inside Estonia," 5.
[160] "Estonia's Defense Industry – Small but InnovativeThis Text Comes from MILMAG Military Magazine. Read More On:https://Milmag.pl/En/Estonias-Defense-Industry-Small-But-Innovative/," MilMag, December 19, 2024, https://milmag.pl/en/estonias-defense-industry-small-but-innovative/.

ensure independence and interoperability across its systems, minimize dependence on foreign contractors, and strengthen Estonian defense.[161] Finally, Desecintl develops land and maritime surveillance systems with a focus on AI implementation across systems. Desecintl highlights the dual-use startup ecosystem in Estonia as its product aims to protect government and private critical infrastructure. These startups all exist at the intersection of entrepreneurship and national security. Defense innovation is not confined to the military but unfolds across local communities, schools, and work places to transform resilience into a national enterprise.

Just as Estonia's comprehensive defense strategy creates a network for Estonians to commit to defending their country, the technological focus of Estonia creates a nervous system through which this whole-of-society system is powered. This is best exemplified by Estonia's fully volunteer-based Cyber Defense League (CDL). Modeled after the Estonian Defense League, the CDL is comprised of high-level cyber analysts who work entirely for free on their own personal time to improve national defense by building cooperation networks for crisis response, improving critical information infrastructure security, and promoting national cyber awareness.[162] The CDL makes defense a professional mission and a civic responsibility. As Estonia's defensive mechanisms have progressed, it has become evident that Estonia is not simply a digitally capable state but a distally resilient society. With every cyber exercise, drone startup, or volunteer, each Estonian and their actions contribute to the shared security fabric.

[161] Ibid.
[162] Mark Grzegorzewski, Margaret Smith, and Barnett Koven, "Civil Cyber Defense – a New Model for Cyber Civic Engagement," *The Cyber Defense Review* 8, no. 3 (2023): 51–66, https://doi.org/10.2307/48755361.

What Does This Mean for Estonian Resilience?

Estonia's model of resilience does not so much as focus on firepower and military capabilities as it focuses on smartness, rapid innovation, and societal integration. Given its deep digital networks, Estonia prides itself in its ability to outthink, outmaneuver, and out-innovate an adversary. Within the equation of Estonian society, EDTs serves as connective lifelines that bind Estonia's civil-military fusion and national commitment to defense. Estonia has found its greater resilience dividends through its distributed innovation.

Estonia does not simply invest in EDT. It develops these technologies within a system where every citizen commits to their part in national defense. Therefore, Estonia treats technical literacy, social cohesion, and defense readiness all as one and the same. Without a technologically literate society, Estonia would cease to be the global hub of innovation it set out to be after its independence. As a result, all of Estonia's resilience rests on the comprehensive mobilization of society around a common defense goal. Under this logic, Estonia cares less about having the best specific form of technology and more about a networked, interconnected society that adapts technology in real time to address the evolving security needs. Through a layered deterrence shell of spikes, with each quill removed from the hedgehog, another spike follows until they are all present or there are none left. The resilience of Estonia as a metaphor to the hedgehog model reveals the importance of projecting Estonia's resilience at an international level. Resilience does not simply serve as an internal precaution. It also serves as an external signal. With each volunteer training, cyber simulation, and drone innovation, Estonia demonstrates that it is far from defenseless. Thus, EDT serves as a tool of communication and national pride.

Russia's 2022 full-scale invasion of Ukraine has reinforced Estonia's commitment to comprehensive defense and resilience. The threats Ukraine faces are not foreign to Estonia; they

are existential by proxy. Ukraine's resilience has fortified Estonian national unity. Ukraine's technological adaptation has empowered Estonians and their drive to participate in civic- and technology-driven defense innovation. Estonia's support for Ukraine stands beyond the symbolic realm. It reflects Estonia's identity as a small, smart state that flourishes through cohesion and not coercion.

Chapter VI: Singapore

Introduction

The following case study will dive into the development of Singapore since its independence in 1965. First, it will explain what makes Singapore a small power. Then, it will trace how Singapore has developed into a Small, Smart Power since its independence through its top-down interventionist approach to government and development. Through its multiple iterations of its armed forces, Singapore has created its defense capabilities from scratch. Singapore has developed a Total Defense approach through which all of Singaporean society is positioned towards defending the nation. Given Singapore's lack of resources, it has focused on making itself a leader in technological innovation. Over time, Singapore has cultivated an ecosystem of militarized civilians who understand their responsibility in creating technology with dual purposes. As a result, Singapore has progressively increased the resilience of the country by spreading a spirit of Total Defense based on constant technological innovation. Unlike the previous two democratic cases of Ukraine and Estonia, where civil society directed the evolution of national resilience, Singapore's semi-authoritarian system focused on state-led and military-centered initiatives.

What Makes Singapore Small?

Singapore, a 721 square kilometer island, is not simply small due to its geographical size but because of its geostrategic vulnerability. Singapore's development has been documented as starting with its unwanted, accidental independence in 1965, followed by a period of having to fend for itself until it was able to develop adequate industries to become economically competitive and militarily secure. With a multi-ethnic population of about 6 million people, Singapore has been conditioned by asymmetries in demography as well as historical legacies and geographical

constraints. On the one hand, Singapore has been blessed. It sits perfectly next to the Strait of Malacca, serving as a link between the Indian and Pacific Oceans. Singapore holds access to more than 40% of world commerce, 50% of world oil, and 80% of oil going to China and Japan, which all pass through the Strait of Malacca and the Singapore Strait.[163] Additionally, Singapore has a deep natural harbor that allows it to serve as a hub for maritime trade, serving as a key portal between Asia, America, Europe, and the Middle East. On the other hand, Singapore is cursed by its geography. Due to its strategic location and lack of natural resources, Singapore is heavily dependent on the outside world. As a single urban hub, Singapore also lacks strategic depth, without anywhere to retreat or a place for citizens to hide in case of an attack, meaning a threat against the island is a threat against the whole nation. As Goh Chok Tong put it, "the loss of one city would mean the loss of the whole nation."[164] Thus, Singapore has seen its biggest national security vulnerabilities as both threatening actions from adversarial neighbors and the general disruption of commerce. Singapore relies on open trade routes and international commerce. Singapore is acutely aware that its security is linked to the great powers who pass through its straits, pursuing their own geopolitical and economic interests. Thus, Singapore has fought to ensure two things: that international actors recognize their vested interest in the continued survival and stability of Singapore and that anyone who threatens its sovereignty and independence will pay a price and face the wrath of the entire nation. Thus, Singapore depends on a strategy of total defense, smart deterrence, and international defense diplomacy to preserve autonomy.

[163] Michael Raska, "The Contours of Singapore's Defence Planning: Rethinking Deterrence, Defence Diplomacy, and Resilience," in *Defence Planning for Small and Middle Powers* (Taylor & Francis, 2024), 45–74, 47.
[164] Kin Wah Chin, "Singapore: Threat Perception and Defence Spending in a City State.," in *Defence Spending in Southeast Asia*, ed. Kin Wah Chin (Singapore: Institute of Southeast Asian Studies, 1987), 194–224, 196.

Steadily Building Smartness

A Rough Road to Independence

After becoming fulling independent in 1965, Singapore bulldozed its way to self-sufficiency and success, never stopping once to turn back on its past. Just five years before it became independent, Singapore had been in a wretched state. The island was full of swamps, swarms of mosquitoes, and vile smells coming from the most densely populated slum in the world at the time. The island lacked plumbing and electricity in most areas, and families lived in tin-roofed houses with up to ten strangers. Clean water was a luxury, and disease ran rampant, with tuberculosis and cholera being the two most common. Infant mortality rates sat at 34.9 deaths per thousand live births, making it the highest in the region.[165] Given the state of Singapore in 1960, it is incredible what Singapore has managed to achieve since its independence in 1965.

Singapore's independence has been described as unwanted, accidental, and unexpected.[166] Singapore's modern history begins in 1819 with the arrival of the British Empire who remained until the 1960s. In 1958, Singapore achieved independence from the British after intense negotiations through the Constitutional Agreement on Independence. Despite becoming politically independent, Singapore still chose to keep British troops on Singaporean soil as they provided a security guarantee against threatening neighbor states, extended close ties with London, and kept the British military base open, which employed a great number of Singaporeans. Singapore, however, still struggled with its newfound independence, so it decided to merge with its next-door neighbor, Malaysia. The decision was based on the logic that joining into a larger state would provide Singapore with a security blanket and a larger market to grow economically and reach its

[165] Sarkissian, *The Small States Club* 18.
[166] Edwin Lee, *Singapore : The Unexpected Nation* (Singapore: Institute Of Southeast Asian Studies, 2008).

full potential. The Malays, however, felt threatened by a surge in Chinese citizens that led to fighting over resources and inflamed racial tensions, and Malaysia expelled Singapore from the larger state only two years after being merged together. This was one of the only times in history when a country has expelled its own constituent state. Humiliated, Singapore suddenly became independent. To add insult to injury, Singapore lost the protection of its British security umbrella after the British announced their withdrawal of troops from all territories east of the Suez Canal in 1967.[167] This withdrawal created a total power vacuum in Singapore as British troops stationed on the island contributed 25% of Singapore's GDP and hired 25,000 locals.[168] As Lee Kuan Yew, Singapore's first prime minister who held this position from 1959 to 1990, stated, "the old era of underwritten security had ended. From now on we had to be responsible for our own security."[169] Thus, Singapore's birth into statehood was defined by successive humiliation and lack of security. Singapore developed a perennial sense of vulnerability, which would fuel its development moving forward.

Lee Kuan Yew faced a daunting task of either resurrecting Singapore from within or letting the island-state wither away. As Lee admitted, the idea of an independent and separate Singapore was "a political, economic and geographical absurdity."[170] Lee's first foreign minister, Sinnathamby Rajaratnam, echoed the same sentiment, claiming that independent Singapore had a near-zero chance of survival, politically, economically, or militarily.[171] Despite these statements, Lee did not give up. Instead, he decided that survival was not sufficient. Lee was ambitiously

[167] P. L. Pham, *Ending "East of Suez"* (Oxford: Oxford Historical Monographs, 2010), 7– 8.
[168] Raska, *Military Innovation in Small States*, 87.
[169] Lee Kuan Yew, *From Third World to First: The Singapore: 1965-2000* (Singapore: Times Publishing Group, 2015), 65.
[170] Andrew Tan, "Domestic Determinants of Singapore's Security Policy," *Asia-Pacific Center for Security Studies*, 2001.
[171] Ibid.

determined to transform Singapore into a leader in the region and role model in the world as a stable, prosperous, secure state.

In contrast to the more decentralized approaches of Ukraine and Estonia, Singapore offers a different story, one in which the state holds absolute control over the state's liberalization and transformation. This spirit of pragmatism was paired with full control over democratic processes, freedoms, and political pluralism, resulting in a one-party state. Lee Kuan Yew used his ends to justify his means. The foundations of Singapore's success arose from centralized, state-orchestrated governance. Lee's administration consolidated executive authority and tightly managed the public sector. Singapore's innovation, security, and identity-building projects were pursued through technocratic planning, dedicated civil service, and harsh political discipline, forming what has often been called a benevolent authoritarianism. Lee Kuan Yew prioritized economic growth and state security over moral and political considerations. He immediately attacked corruption, rooting it out from traces of Singapore's colonial economic model. Corrupt officials were stripped of immunity, the judiciary authority revoked any illicit gains, and salary increments were introduced to prevent corruption among public servants. As a result, a deep spirit of personal integrity and accountability spread among society and formed national Singaporean values

Lee set the foundation for Singapore by crafting a national Singaporean identity. Given that Singapore lacked a national, ancient history, Lee created a story of the state that did not look back on the past but looked forward to the future. Lee first addressed ethnic tensions between the large Chinese, Malay, and Indian communities that lived in Singapore. To this day, Singapore is incredibly diverse. As of 2023, 3.61 million Singaporeans of the total population of 5.9 million

people had a Chinese background.[172] The multicultural mix can be broken down into 75% Chinese, 14% Malaysian, and 9% Indian and a religious diversity consisting of Buddhism, Islam, Christianity, Judaism, and Hinduism.[173] Lee created a culture based on ethnic equality where all were Singaporean before all else. Lee turned what could have been perceived as Singapore's greatest weakness into its foundational strength. As Rajaratnam explained, Singapore would not allow its "cultural differences" to lead to "cultural cannibalism."[174] Instead, this multiethnic makeup would serve to produce "intellectual enrichment" and national pride.[175] Setting the goal for Singapore as a booming economy, advanced industries, a powerful military, and a thriving, educated society, Lee also had to accept that he was starting from practically nothing. Thus, Lee approached his plan with flexibility and a willingness to revise and rethink ideas. Lee balanced his idealistic goals for Singapore's development with a strong spirit of pragmatism.

Lee looked to various sources to build Singapore's national culture. Western rigidity was mixed with traditional Asian values to establish individualism, thrift, diligence, and deference to authority as fundamental values of the Singaporean citizen.[176] Lee pulled from the Indian concept of unity in diversity and the American mantra of *E Pluribus Unum* to create a single nation not defined by ethnicity but by citizenship. A state housing program exemplified this notion by creating affordable housing to provide Singaporeans with a basic necessity and a base from which Singaporeans could then pursue work. The program also contributed to breaking down ethnic difference and building this singular Singaporean identity by encouraging the cohabitation of the three main ethnic groups in each neighborhood.[177]As a result, ethnic enclaves were avoided and

[172] Raska, "The Contours of Singapore's Defence," 48.
[173] Sarkissian, *The Small States Club*, 28.
[174] Ibid, 22.
[175] Ibid, 22.
[176] Sarkissian, *The Small States Club*, 27.
[177] Ibid, 29.

schools, shops, and communities were automatically multiracial environments. The introduction of mandatory military service also forced the multiethnic society to put their previous national identities behind and commit to defending Singapore together. As Singaporean leaders saw it, conscription would help "break down the barriers of communalism" by providing "opportunities for Singapore youths to acquire a sense of commitment to the nation."[178] These initiatives were not meant to erase past ethnic backgrounds. They worked to create a civic idea of citizenship that promoted a unified nation which celebrated and appreciated cultural diversity. Singapore invited immigrants who were talented and willing to embrace Singaporean values, coexist with other cultures, and actively participate in the collective progress of the nation. The success of Lee's strategy is reflected by the fact that 95% of residents in Singapore identified as Singaporean in 2015.[179] From this collective identity, Lee institutionalized this cultural and political imperative into Singapore's defense and security.

1G SAF – The Poisonous Shrimp that Learned to Walk Before It Could Run

In the first decade of its existence, Singapore focused on survival. Lee Kuan Yew and his political officials had to build the Singaporean Armed Forces (SAF) from the ground up, creating defense planning, organizational structure, doctrine, training concepts, and weapons procurement out of nothing. To coordinate this massive task, the Ministry of Defense (MINDEF) was established in 1965 to oversee defense policy, military strategy, and technological development. Singapore realized that hard power alone could not guarantee survival. With limited manpower and zero strategic depth, Singapore had to adopt asymmetric strategies—developing force multipliers

[178] Charles Edward Morrison and Astri Suhrke, *Strategies of Survival: The Foreign Policy Dilemmas of Smaller Asian States*(Australia: University of Queensland Press, 1978), 175.
[179] Sarkissian, *The Small States Club,* 30.

through advanced training, careful force structuring, and pragmatic technology acquisition. This laid the groundwork for a future military model built not on size, but on adaptability and innovation—early indicators of smartness.

Known as the First Generation of the SAF (1G SAF), this period focused primarily on developing basic capabilities. In October 1965, the Ministry of the Interior and Defense (MID) was formed followed by the creation of the Singapore Armed Forces Training Institute (SAFTI) in February 1966 to train all officers and non-commissioned officers.[180] On February 27, 1967 the National Service (Amendment) Bill was passed, making all males eligible for military call-up after their 18th birthday.[181] The introduction of the bill rapidly expanded the SAF from 2,000 troops in 1967 to 14,000 in 1970 to 25,000 in 1975.[182]

The SAF was not born from colonial or previously standing armed forces that were tied to the political ruling elite like in the cases of Ukraine and Estonia. Instead, the SAF was born from scratch and came out of an ad hoc effort to create a defense force in a country where very few people had any military experience. Not built by experienced veterans, the SAF was built by civilian administrators like Goh Keng Swee, the country's finance minister in its first cabinet, who took on positions of military leadership.[183] A direct influence of this development was that the SAF took on a unique form of civil-military fusion that created a society of military civilians. This model of the militarized civilian was reinforced by subsequent decades of public discourse reminding citizens and non-citizens of their duty to defend Singapore.

---

[180] Raska, *Military Innovation in Small States*, 76.
[181] Ibid, 76.
[182] International Institute for Strategic Studies. 1967–1975. *The Military Balance* 1967, 1970, 1975. London, UK: IISS.
[183] Shannon A Brown, "Singapore: Civil- Military Fusion and Militarized Civilians," in *The Routledge Handbook of Civil- Military Relations*, ed. Florina Cristiana Matei, Carolyn Halladay, and Thomas C. Bruneau (New York: Routledge, 2021), 118–30, https://doi.org/10.4324/9781003084228-11, 120.

The early development of the SAF was heavily influenced by Israel and the Israeli Defense Forces (IDF). Singapore turned to Israel for help as then Prime Minister Lee Kuan Yew and Defense Minister Goh Swee believed Israel could help Singapore create a "small, dynamic army" given that it was surrounded by Muslim countries just like Singapore.[184] The SAF's embrace of Israeli doctrine was not just about tactical training. It represented a strategic replication of a small state innovation model. Like Israel, Singapore internalized the concept that survivability comes from technological edge, rapid mobilization, and operational flexibility—key signs of a smart military.

While building its defensive capabilities, Singapore based its first defining strategic pillar on deterrence. Singapore set its top priority as building a self-reliant military while also creating credible deterrence. This strategy was largely shaped by the threat perceptions of the time, fearing that Malaysian and Indonesian power might hurt Singapore. For example, Malaysia made multiple threats to cut off water supplies to Singapore setting the conditions for the development of SAF's air and land powers.[185]

From the early 1970s until the mid-1980s, Singapore based its defense model on the "Poisonous Shrimp" strategy. Lacking the defense capabilities to defend the island, the SAF decided on a strategy of using high-intensity combat to impose unimaginable human and material costs. The SAF weaponized the city-state on the basis of powerful symbolic images.[186] The poisonous shrimp model was based on the analogy of "easy to swallow but impossible to

[184] Raska, *Military Innovation in Small States*, 77.
[185] Bernard Fook Weng Loo, "Explaining Changes in Singapore's Military Doctrines: Material and Ideational Perspectives" in Asia in the New Millennium: APISA First Congress Proceedings, 27-30 November 2003, edited by Amitav Acharya and Lee Lai To (Singapore: Marshall Cavendish Academic, 2004), 352-375, 367.
[186] Antony Dabila and Thibault Fouillet, "What Is Small-State Security Policy?," *Routledge*, September 12, 2023, 118–35, https://doi.org/10.4324/9781003356011-10, 131.

digest."[187] With its lack of manpower, mobility, and strategic depth, Singapore acknowledged that it could not resist an invader, so it made it clear that the cost of victory would mean the total destruction of both Singapore and the adversary. The strategy was combined with an agreement that British, Australian, and New Zealand forces would provide assistance through the Fiver Power Defense Arrangement (FPDA); however, Singapore was left mostly on its own after the FPDA was scaled down during the 1970s.

A key flaw in the "Poisonous Shrimp" strategy is that admits defeat even before fighting starts. While it promises great pain onto the invader, it guarantees defeat.[188] As Brig. Gen. Lee Hsien Loong, then the Chief of Staff of the SAF, put it, "the Poisonous Shrimp strategy was deficient in that it offered Singapore merely a choice of 'suicide or surrender' because of its implication that the SAF would fight an ultimately unwinnable war on its own territory."[189] While assuming the "Poisonous Shrimp" strategy, Singapore continued to develop and modernize the SAF. At the strategic level, it continued to pursue deterrence by finding ways to create strategic depth and move the forward edge of the battle line area away from its urban city and waterfront leading to a new strategy by the middle of the 1980s.

2G SAF: The Porcupine and The Introduction of Total Defense

The Second Generation (2G) SAF graduated from the "Poisonous Shrimp" model to the "Porcupine" model. Under this analogy, Singapore's developed small but painful spikes would offer protection at a greater distance. This switch reflected the development of Singapore's defense

[187] Bilveer Singh, *Arming the Singapore Armed Forces (SAF)): Trends and Implications* (Canberra: Strategic and Defense Studies Center, ANU, 2003), 26.
[188] Loo, "Explaining Changes in Singapore's Military Doctrines," 367.
[189] Tim Huxley, *Defending the Lion City: The Armed Forces of Singapore* (St. Leonards Australia: Allen & Unwin, 2000),57.

capabilities which were more offensive and survivable. The "Porcupine" strategy required military capability, military planning capacity, and the ability to project defense both internally and externally.[190] The SAF was no longer focused on just developing individual services but began experimenting with new planning and execution doctrines at the system level. This led to the introduction of the Total Defense concept in 1984. The Total Defense doctrine reflected a shift from survival to smartness. Tt conceptualized defense as a multi-domain challenge based on military, social, economic, psychological, and later digital defense. Total Defense approach demonstrates an early articulation of Singapore's whole-of-society asymmetric defense, in which societal integration and technological adaptation generate resilience rather than sheer military scale or technology.

With the introduction of the Total Defense concept, Singapore made it a core feature to indoctrinate the population to have a preparedness mindset.[191] It mobilized all of Singapore and its resources towards increasing the resilience, readiness, and resolve of every sector of society. Initially, Total Defense was made up of five pillars: military defense, economic defense, civil defense, social defense, and psychological defense. A sixth pillar of digital defense was introduced in 2019 which will be discussed later on in this section. All the pillars were united under the greater goal of uniting all Singaporeans under the joint goal of defending the nation justified by the Singapore's small size, lack of national resources and manpower, and its ethnically diverse population.[192] Making the defense of Singapore a comprehensive whole-of-society concern in times of war and peace, Total Defense has become a symbol of Singaporean identity based on the

[190] Pak Shun Ng, *From "Poisonous Shrimp" to "Porcupine": An Analysis of Singapore's Defence Posture Change in the Early 1980s* (Canberra: National Library of Australia, Strategic and Defence Studies Centre, 2005), 1–58, 33.
[191] Brown, "Singapore: Civil- Military Fusion," 122.
[192] Ron Matthews and Fitriani Bintang Timur, "Singapore's 'Total Defence' Strategy," *Defence and Peace Economics* 35, no. 5 (March 9, 2023): 638-658, https://doi.org/10.1080/10242694.2023.2187924, 642.

domestic defense industrial base. The military pillar is built on Singapore's military-industrial complex. Singapore's defense industrialization began in 1967 soon after the country's independence. As its indigenous defense industry grew first producing basic capabilities during 1G SAF, 2G SAF saw the consolidation of multiple branches and the establishment of the state-owned ST Engineering (ST Engg) in 1994.[193] ST Engg is divided into four branches: ST Aeropsace, St Marine, ST Electronics, and ST Kinetics. This growing defense-industrial base showed an increased capacity and a transition toward industrial adaptation. By directing state-owned enterprises like ST Engineering to absorb foreign technologies via offset agreements and develop indigenous capabilities, Singapore set the foundation for a model of strategic self-reliance powered by smart technology acquisition and development.

During this 2G SAF period, spending on defense research and development (R&D) increased substantially. While 1% of defense spending went toward R&D in 1990, this grew to 4% by 2000, marking an increase from $20 million to $160 million in real terms.[194] Another part of this military pillar is Singapore's national service requirement. By forcing all eligible men to serve in the SAF, Singapore has formed a national identity that surpasses ethnic, class, religious, or ideological differences. The ideas of universality and equity that come from National Service (NS) trickle into Singaporean society, strengthening social resilience against any possible threat to stability. This top-down approach to national defense is emblematic of Singapore's broader governance model. Citizens participate in society and are ingrained into state-mandated structures that define national responsibility and cohesion. Singapore's Total Defense strategy is thus less a

[193] Matthews and Timur, "Singapore's 'Total Defence' Strategy," 644.
[194] Bernard Fook Weng Loo, "The Management of Military Change: The Case of the Singapore Armed Forces," in *Security, Strategy and Military Change in the 21st Century*, ed. Jo Inge Bekkevold, Ian Bowers, and Michael Raska (Routledge, 2015), 70–88, 79.

grassroots phenomenon and more a state-enforced societal position, where the government sets the agenda and mobilizes all sectors of society to execute it.

Just as Singapore relies heavily on its ability to defend itself, this ability to sustain its security, the military pillar that is, depends on the economic pillar. The economic pillar is vital to the resilience of Singapore. Without a strong economy, the costs of creating, maintaining, and innovating effective security capabilities would be too high. Singapore serves as a testament to the interdependence of military power and economic strength. Lacking self-sufficiency, Singapore has integrated into the global economy. As former Defense Minister Teo Chee Hean quoted Sir Shridath Ramphal, former secretary general of the Commonwealth, claiming that Singapore is like a small boat "pushed out into a turbulent sea, free in one sense to traverse it; but without oars or provisions, also to perish. Or perhaps to be rescued and taken aboard a larger vessel."[195] To compensate for the shocks of the international arena's waves, Singapore has taken an interventionist, non-dependent approach to economic, industrial, and technological development in order to meticulously select responses to these shocks. Singapore has used its economy as another source for social cohesion. Positioning the survival and defense of the nation on the military and then making it clear that the military depends on the economy, Singapore has ingrained into the minds of its citizens that their contribution to the economy is necessary for the survival of the state. Every job has been angled towards the defense of the nation. Singapore has promoted this idea of a "stakeholder society" where every aspect of life contributes to national defense.[196]

---

[195] Ahmed S. Hashim, "Security & Defense in Small States: Qatar, the UAE and Singapore," *Middle East Policy* 27, no. 3 (September 2020): 30–45, https://doi.org/10.1111/mepo.12511, 40.
[196] Beng-Huat Chua, *Political Legitimacy and Housing: Singapore's Stakeholder Society* (London: Routledge, 2002).

The civil, social, and psychological pillars further reinforce this militarized civilian pattern of thinking. Civil defense covers Singapore's police force as well as systems to address national crises. It provides basic needs like training for rescue work, evacuation procedures, shelter management, first-aid, and damage control in order to maintain confidence and resilience throughout society regardless of the national crisis.[197] The social pillar aims to promote social cohesion, harmony, and tolerance between Singapore's diverse ethnic groups in order to maintain and strengthen national unity and stability. As defined by the Singaporean government, the social pillar is an "effort to understand differences between distinctive races and cultures, so that all segments of society are united under the same flag."[198] Finally, psychological defense aims to foster a collective will to commit to ensuring Singapore's independence. Arguably the most important pillar of Total Defense, psychological defense creates a sense of trust among Singaporeans to believe in societal and government instructions and be resilient in the face of unexpected crises. Through initiatives like National Education Programs required in schools, the goal is to foster a sense of belonging and national pride, empowering all Singaporeans to develop the confidence, courage, and collective will to rapidly mobilize and remain resilient in the face of crisis.

As 2G SAF evolved, the concept of Total Defense was transformed into the broader idea of Total Security. Total Security introduced the idea that defense planning was not just about technology, innovation, and integration but also required cooperation with neighbors and friends. Total Security combined the internal stability aspect of the social, civil, and psychological pillars of Total Defense which emphasizes social cohesion and harmony with the broader global

[197] Singapore Ministry of Defence, "News Release: Factsheet - about Total Defence," 2004, https://www.nas.gov.sg/archivesonline/data/pdfdoc/MINDEF_20040207001_2/MINDEF_20040207003.pdf.
[198] Singapore Ministry of Defence, "Total Defence," 2024, https://www.mindef.gov.sg/defence-matters/defence-topic/total-defence.

understanding of Singapore's need to establish itself within the international system which came from the economic pillar. This gave birth to the three-dimensional "S-Cube Concept" presented in a 1995 defense white paper which declares survival, security, and success as the foundation of Singapore's future.[199] As Lee Kuan Yew would later state during a lecture in 2009 at the MFA Diplomatic Academy, "a small country must seek a maximum number of friends while maintaining the freedom to be itself as a sovereign and independent nation. Both parts of the equation– a maximum number of friends and freedom to be ourselves– are equally important and inter-related."[200] Defense diplomacy serves as a way for Singapore to create and deepen bilateral and multilateral defense dialogue and cooperation agreements. Singapore has close ties with various countries such as the ASEAN states, the United States, China, South Korea, New Zealand, and India. Through these agreements, Singapore creates bonds of trust with other nations, strengthening Singapore's position regionally and globally while contributing to the defense of other states. Thus, Total Defense also creates a node connecting development, deterrence, and diplomacy from which Singapore unites its citizens together and lets its smartness flourish. By the early 2000s, Singapore's defense planners realized that a robust, structured, resilient society was not adequate in a world of ever-changing threats. A new generation of the SAF was required to usher Singapore towards digital transformation, networked warfare, and strategic foresight– finalizing the full maturation of Singapore's smart state identity.

[199] Raska, *Military Innovation in Small States*, 86.
[200] Yew, Lee Kuan. "The Fundamentals of Singapore's Foreign Policy: Then & Now." Presented at the S. Rajaratnam Lecture at MFA Diplomatic Academy, May 9, 2009. https://www.pmo.gov.sg/Newsroom/speech-mr-lee-kuan-yew-minister-mentor-s-rajaratnam-lecture-09-april-2009-530-pm-shangri.

3G SAF – The Smart Dolphin Dives Into Smartness

Launched in the early 2000s, the Third Generation (3G) SAF marked Singapore's most comprehensive transition to a smart defense posture. It marks a transformative shift both technologically and socially as EDT like AI, cyber, autonomous systems, and cyber were fused into society through the pre-existing Total Defense framework. On March 15, 2004, then Minister of Defense Teo Chee Hean gave a speech known as the "Statement at the 2004 Budget Debate in eh Singapore Parliament" where he called for Singapore to transition from simply being operationally ready to developing future oriented capabilities in order to adapt to the rapidly changing challenges of the future.[201]

Building from Total Defense and development of an indigenous defense industrial base, 3G SAF introduced advanced technological integration and organizational agility into Singapore's military. Technology has since been labeled a critical force multiplier and been the focus of every development.[202] Singapore no longer focuses on deterring or delaying an adversary. Transitioning from the "Porcupine" model to the "Smart Dolphin" model, Singapore has worked to out-think and outmaneuver enemies through smart, coordinated, technologically superior means. Since the start of 3G SAF, the battlespace expanded beyond air, space, and land to include cyber, information, and space. The switch to the "Smart Dolphin" was analogous to an embrace of the small, smart power model. Singapore began focusing on intelligence, speed, and maneuverability at all levels of the military and society.

The SAF's 3G transformation reflects the expanding range of threats that are present today, ranging from terrorism to disinformation, from conventional war to hybrid war, from climate

[201] Teo Chee Hean, "Statement at the 2004 Budget Debate in the Singapore Parliament," Parliamentary Debates Official Report - Tenth Parliament.
[202] Tim Huxley, "Singapore and Military Transformation," in *The RMA for Small States: Theory and Application* (Singapore, 2004), 2.

change to pandemics. In this 3G of SAF, Singapore has shifted to penetrating the fog of these ever-widening risks and anticipating the next threat through strategic foresight.[203] Each agency was given a foresight team like MINDEF's Security and Intelligence Division (SID) or the Center for Strategic Futures of the Prime Minister's Office.

Under this 3G SAF, technology has been the paramount point of focus. This led to the introduction of a Revolution in Military Affairs (RMA) framework of thinking within the SAF. After studying the U.S. experience in the Gulf War and the RMA debates which arose from the conflict, Singapore adopted the RMA concept as a way to develop technological advancements and gain a strategic edge. This RMA mindset embraced small arms, networks, enhanced command control systems, and digitally focused approaches to warfare.

This led to the SAF and Singapore finding new doctrines which embraced operational flexibility and agility. Based on a series paper published by the Singapore Armed Forces Training Institute (SAFTI) titled *Creating the Capacity to Change (2003); Realizing Integrated Knowledge-based Command and Control – IKC2 (2003); and Spirit and System: Leadership Development for a Third Generation SAF (2005)*, the SAF shifted its development from linear projections based in the present to embracing nonlinear concepts based on the capacity to change and innovate quickly.[204] MINDEF outlined emerging discontinuities in genetics, biometrics, computing power, broadband data communications, GPS, precision-guided munitions, robotics, nano-technology, the rise of nonstate actors, and the effects of globalization as the biggest threats in the 21st Century. The SAF recognized its own deficiency in its bureaucratic, organizational resistance to change which stemmed from its top-down, state-controlled structure and pragmatic, selective approach to innovation and integration. The SAFTI reports called for the SAF to restructure itself to allow for

[203] Raska, "The Contours of Singapore's Defence," 45.
[204] Raska, *Military Innovation in Small States*, 88.

creativity and innovation to flow naturally through the SAF and Singapore as a whole.[205] With the beginning 3G SAF, MINDEF committed to a technologically-integrated operations (*Ops-Tech)* innovation strategy that connected defense technology users, the SAF; developers, science and technology base; and producers, the defense industry. Through *Ops-Tech*, Singapore stressed that innovation and technological integration was not simply about strengthening the SAF but fully weaving Singaporean society together to become more resilient

In order to implement this 3G SAF transformation, MINDEF introduced new organizations to drive radical change and innovation. The creation of these branches transformed the whole-of-society approach which Singapore had built over time, from slowly developing technology to being fully technologically facing. Singapore had previously ingrained this technological prioritization into its culture of civil-military fusion through the creation of various organizations during 1G SAF and 2G SAF. For example, in 1971, Singapore's first defense minister Goh Keng Swee created the Electronic Warfare Study Group, also known as the Electronics Test Center (ETC). Staffed with 5,000 defense scientists, engineers, acquisition professional, and logisticians, ETC created an early base for civil-military innovation that would serve as the foundational base for Singapore's vibrant defense technology ecosystem.[206] Similarly the MINDEF Defense Tech Group (DTG), which was originally established in 1986, oversees all research and design (R&D). DTG oversees research on EDT like AI, robotics, unmanned vehicles, cyber security, and advanced materials; partnering with academia through universities, research institutes, and private companies; helping the SAF discover, test, and adopt new technology into its operations; and developing expertise by growing and attracting skilled talent.[207]

---

[205] Dawen Choy, Ju-Hon Kwek, and Chung Han Lai, *Creating the Capacity to Change: Defence Entrepreneurship for the 21st Century* (Singapore: SAFTI Military Institute, 2003), 16.
[206] Teo Chee Hean, "Speech by Mr Teo Chee Hean, Minister for Defense," Ministry of Defense Singapore.
[207] DSO National Laboratories, "Our History," DSO National Laboratories, 2024, www.dso.org.sg/about/history.

Launched on November 5, 2003, the Future Systems Directorate (FSD) was initially given 1% of the overall defense budget to innovate, experiment, and produce change based on alternate concepts and disruptive technology.[208] This was followed by the creation of the Defense Research and Technology Office (DRTO) in 2006 to merge pre-existing research and technology (R&T) planning and management teams into a single agency which planned and managed the direction of R&T. In 2013, MINDEF merged FSD and DRTO to create the Future Systems and Technology Directorate (FSTD) to structurally entrench their expertise into a unified pursuit of innovation.[209] Today, FSTD is one of four departments of MINDEF focused on technological innovation which also include the Technology Strategy & Policy Office (TSPO), the Industry & Resources Policy Office (IRPO), and the Defense Technology Collaboration Office (DTCO).[210] The whole Defense Tech Group is supported by a broader level by the Defense Tech Community (DTC) which integrates three technology research arms: the Defense Science and Technology Agency (DSTA), which aims to grow Singapore's community of engineers and scientists from civil society and academia; DSO Labs—Defense Science Organization, which is Singapore's largest defense R&D organization; and the Centre for Strategic Infocomm Technologies (CSIT), which focuses on cybersecurity, data analytics, software engineering, and cloud infrastructure and services.[211] As an example of deliberate initiatives to create national security collaboration throughout Singaporean society, DSTA started the Open Innovation Platform and DSTA BrainHack, which engages with students, researchers, and civilian tech creators to co-produce defense solutions using EDT. DSTA BrainHack has worked with over 4,000 students from 109 schools across Singapore, working on

[208] Jimmy Khoo, "Keynote Address by Future Systems Architect, BG Jimmy Khoo at C4I Asia Conference," Ministry of Defense Singapore.
[209] Raska, *Military Innovation in Small States*, 92.
[210] Ministry of Defense Singapore, "Defence Science & Technology," MINDEF, 2024, https://www.mindef.gov.sg/defence-matters/defence-topic/defence-science-technology.

[211] Raska, "The Contours of Singapore's Defence," 56.

cybersecurity, AI, unmanned systems, and space tech.[212] Through public engagement, Total Defense becomes more than just a state-enforced doctrine. It invites citizens to innovate through collaboration, enhancing the civilian tech ecosystem just as much as the military domain. Thus, national resilience is increased as defense becomes a shared responsibility as opposed to solely a government project.

Singapore's innovation and technological development have long been based on a spirit of civil-military fusion that prioritizes the creation of dual-use technology. Since 1977, the Defense Sciences Organization (DSO) has integrated into the commercial sector to create a comparative advantage for Singapore. Originally focused on electronic warfare, DSO has expanded its focus to dual-use technologies like artificial intelligence, electro-optics, communications, and software engineering. DSO has been integrated into the commercial sector through two main developments. First, the Singaporean government committed to incorporating its national science and technology bases into its indigenous SAF R&D muscle. The Singaporean government applied its interventionist approach to economic development to further fuse the commercial sector with the SAF through the 1991 Strategic Economic Plan. The plan set out to enhance education and training, generate international focus through greater outward investment, increase innovation by paying greater attention to R&D, and support industrial and technological clusters, which would simultaneously spur rapid economic growth and bolster Singaporean security and defense. Additionally, the National Science and Technology Plan, released in 1996, complemented this interventionist approach to civil-military melding. Proposing a $2.36 billion Five Year Programme, the plan strove to turn Singapore into a R&D hub by hiring 65 researchers per 10,000 workers.[213]

[212] Singapore Defence Science and Technology Agency, "Imagining What's Next," DSTA, July 4, 2025, https://www.dsta.gov.sg/whats-on/spotlight/imagining-what.
[213] Matthews and Yan, "Small Country 'Total Defence,'" 389.

Thus, the plan simultaneously fostered innovation of technology which could be implemented into the SAF and also grow Singapore into a world leading science and technology hub. Second, Singapore commercialized DSO pulling it out of the traditional government echo-chamber into a interconnect, networked organization. Beginning in 1997, DSO began its commercialization as it became DSO National Laboratories followed by being merged into the Defense Science and Technology Agency (DSTA) by 2000. As DSO evolved, it became leaner and cut red tape, allowing for greater collaboration with academia and private sector companies.

The SAF has also found a way to merge old technology with new innovations through ST Engg. As of 2019, ST Engg employed nearly 23,000 workers globally and generated US$5.73 billion in total revenue.[214] As Singapore has pursued a technologically-driven militarized society, it has not solely relied on homegrown technology. Singapore has exploited its high-tech engineering and dual-use industrial capability to meet both commercial and military demand.[215] The country has imported systems from allies and revamped them with new indigenous technology. With few resources, the SAF has remained cost-effective, not just developing new technology but also integrating new technology into old weapons systems.

Thus, Singapore has indoctrinated the entirety of its society towards producing and innovating technology which can improve its military capabilities and therefore increase its defense and security. By militarizing citizens towards this Total Defense techno-mindset, Singapore has created a "techno-anxiety"-driven socio-industrial culture that Singaporeans are born into.[216] This mindset

[214] Richard A. Bitzinger, "Military-Technological Innovation in Small States: The Cases of Israel and Singapore," *Journal of Strategic Studies* 44, no. 6 (July 21, 2021): 873-900, https://doi.org/10.1080/01402390.2021.1947252, 887.
[215] Ron Matthews and Nellie Zhang Yan, "Small Country 'Total Defence': A Case Study of Singapore," *Defence Studies* 7, no. 3 (September 2007): 376–95, https://doi.org/10.1080/14702430701559289, 388-389.
[216] Alan Chong, "Smart City, Small State: Singapore's Ambitions and Contradictions in Digital Transnational Connectivity," *Journal of International Affairs* 74, no. 1 (2021): 243-60, https://www.jstor.org/stable/27169782, 218.

has been reinforced through campaigns like the 2014 "Smart Nation" initiative and the "Smart Country 2025 Plan" which promise to maximize the use of technology to improve the lives of citizens, connect businesses with the government, and increase security of Singapore.[217] Singapore wants the "Everything and Everybody Everywhere All the Time" notion to unify Singaporeans on a foundation of technological development in order to maximize the survival of the nation.[218] These policies and a push to make Singapore a "Smart Nation" are met with high levels of public participation. High buy in into digital projects like TraceTogether, SafeEntry, and the National Digital Identity (NDI) reveals societal trust in technology, enhancing collective security. By 2021, for example, over 90% of Singaporeans had registered with TraceTogether to contact trace for COVID-19.[219] This pursuit of smartness led to the addition of a sixth digital pillar in 2019 to the Total Defense concept. The digital defense pillar serves to protect critical infrastructure and systems from cyber threats, build cybersecurity specialization, and promote responsible internet use. It formalized the role of every citizen in defending the nation digitally. The creation of this pillar was followed by the establishment of the Digital and Intelligence Service (DIS) as the fourth branch of the SAF, adding to the military, navy, and air force. These new structures in addition to initiatives which incentivize citizens, businesses, and public groups to participate in national defense all solidify the idea that resilience and defense require the whole-of-society.

[217] Ning Wang, "Singapore's Experience and Enlightenment of Building a 'Smart Nation,'" ed. K.H.M. Mansur and Y. Fu, *E3S Web of Conferences* 251 (2021), https://doi.org/10.1051/e3sconf/202125101069.
[218] Esra Banu Sipahi and Zabihullah Say, "The World's First 'Smart Nation' Vision: The Case of Singapore," *Smart Cities and Regional Development Journal* 8, no. 1 (2024): 41–58, 44.
[219] Cara Wong, "Budget Debate: Contact Tracing Process Shortened with Almost 90% of S'pore Residents Using TraceTogether," The Straits Times, February 26, 2021, https://www.straitstimes.com/singapore/politics/almost-90-per-cent-of-residents-on-tracetogether-programme.

What Does This Mean for Singaporean Resilience?

Unlike Ukraine and Estonia's largely bottom-up defense approaches to total defense, Singapore has engineered resilience through EDT integration into total defense from the top down. Despite the differences in philosophy, Singapore has created deep resilience by combining state planning with civil-military fusion which dates to the birth of the nation. Its citizens thrive on a "ready to fight mindset" in order to deter any potential predators.[220] Through this whole-of-society, smart strategy, Singapore has turned its geopolitical and geo-strategic vulnerability into power and capability.

Singapore has created a deterrent force through merging technological sophistication with societal dedication to survival. EDT has allowed Singapore to function at an operational level beyond that which the nation's size would suggest. At the same time, total defense has mobilized the entire country to support this small state pursuing big dreams. Throughout its journey from "Poisonous Shrimp" to the "Porcupine" and ultimately to the "Smart Dolphin," Singaporeans have been crafted a digitally-forward, security-maximizing society. Singapore's evolution to the "Smart Dolphin" concept today reflects the growth of a small power that is now able to innovate new concepts in the face of rising hybrid war threats. It reveals a state that has harnessed smartness to an extent where it now focuses on Operations Other Than War (OOTW).[221] The SAF has harnessed EDT like drones, AI, and autonomous systems to prepare for and deter conventional threats but also expand the horizon of its foresight to hybrid, cyber, natural, and even societal disruptions, creating resilience against attack and also disintegration from within.

[220]Hashim, "Security & Defense in Small States," 40.
[221] Loo, "The Management of Military Change," 80-83.

Singapore's greatest current threat to its total defense posture and resilience is its shrinking demographic profile. Said to be a "demographic time bomb," Singapore has hit historic lows in population growth.[222] Due to both previous government policies controlling rapid growth and a general reluctance from younger generations to have children due to Singapore being one of the most expensive cities in the world, the fertility rate hit a historic and world low of 0.97 in 2024, falling far below the needed replacement rate of 2.1.[223] By 2030, it is estimated that the man-power supply for the NS will decrease by a third.[224] Given the manpower shortage, Singapore needs to maintain its smart strategy and remain innovative. Singapore will need to creatively change existing rules and structures to adapt its strategic culture in order to respond to the nation's demographic problem. In order to remain resilient, Singapore ultimately has no other choice but to look to technology as its greatest strength and best solution to future problems.

[222] Hashim, "Security & Defense in Small States," 42.
[223] Natasha Ganesan, "Singapore's Total Fertility Rate Falls to Historic Low of 0.97," CNA, February 28, 2024, https://www.channelnewsasia.com/singapore/singapore-total-fertility-rate-population-parents-children-4155616.
[224] Raska, "The Contours of Singapore's Defence," 48.

Chapter VII: Conclusion

This thesis has attempted to add to a growing discussion on the topic of small powers and their ability to influence an increasingly splintering international system. The days of the Cold War bipolarity and subsequent moment of U.S. unipolarity have faded, and states are finding themselves both more responsible for their own survival and with a wider range of options in order to ensure said survival. This thesis set out to answer the following question: how does EDT impact the resilience of small powers? The thesis followed the causal pathway that EDTs offer a small power with capabilities that do not require intense physical resources, can be transformed into a dual-use function, and may serve as a force multiplier. By innovating domestic EDT and integrating it into defense and civil systems, a small power may increase its resilience by embedding it across strategic, societal, and operational levels of defense.

In asking this question, this thesis has found that resilience is home-grown and relational. It is not something that can be inserted externally but must grow over time and disperse in times of crisis or existential threat through a web of relations. This realization and the case studies presented above have caused the reconsideration of EDT as the prime influence resilience. Instead, it seems that total defense, or a comprehensive whole-of-society approach, is the stronger causal pathway to increasing resilience. In all three cases, it appears that a total defense doctrine based on *smartness* creates a more resilient society where all citizens are aware of, deeply integrated into, and fully involved in defending their state. The small, smart state uses technological innovation to reinforce total defense, which commits all of society to defense, thus making the society more resilient.

In all three cases, these countries had to reinvent themselves due to varying circumstances. That said, all three states have had to deal with ethnically diverse populations.

While Estonia and Ukraine have large Russian-speaking communities, Singapore has a wide spread of ethnic backgrounds, although notably Chinese-dominated. In all cases, these diverse backgrounds presented problems to national unity at different points in the respective country's development.

The conditions for growth were based on necessity and the need for survival. Ukraine, in the aftermath of its post-Soviet independence, has had to fight for its survival against multiple direct military confrontations with Russia. While the Euromaidan Revolution and annexation of Crimea in 2014 served as initial sparks for change, the 2022 Russian full-scale invasion of Ukraine has been the full catalyst that has pushed Ukraine into an overdrive for existentialist innovation and adaptation. Estonia, which was also presented with a multiplicity of development options to pursue after the collapse of the Soviet Union, gambled its future by pursuing total innovation that had never been unseen before. Instead of taking a classical approach of immediate shelter under either a Western or Russian alliance, Estonia pursued independence and self-sufficiency based on digitalization and technology. While Estonia joined NATO and the EU in 2004, it remained committed to maintaining independent defensive capabilities, always wary of the commitments of collective defense. The 2007 cyberattacks are a testament to Estonia's commitment to indigenous defensive capabilities, as the crisis led to a full commitment to total defense. Finally, Singapore, which was left in a security vacuum when released by its security guarantor in the Britain as well as humiliated by Malaysia, had to fend for itself and develop its own national image, economy, defense, and strategic vision for its future. While Estonia's model focuses on digital governance and cyber-powered civil readiness, and Ukraine's model has evolved into a society-led defense-tech ecosystem powered by decentralization and digital tools, Singapore's approach offers an alternative example of this smart, whole-of-society mindset through top-down control.

The comparison also presents an evolutionary pattern that emerges across the small, state model. The development of these countries seems to follow a transition in the defense and security doctrine of Singapore, starting with the transition from poisonous shrimp to the porcupine and finally ending with the smart dolphin strategy. Singapore, whose case study provides the most extended time period for analysis, has mapped the evolution across all three stages of small, smart state strategy. As it seems, as the small, smart state evolves and its technological foundation grows, it passes through the stages of evolution in defense strategy, gaining greater adaptability and foresight into a wider range of threats. This establishes Singapore as the smart dolphin with the potential to offer a new model with its next evolution. Estonia and Ukraine appear to offer something closer to the porcupine, or hedgehog as Estonia titled itself.

Despite their differences, all three cases recognize that in an era of hybrid threats, smartness, founded on technological innovation, agility, and whole-of-society mobilization, is the most powerful defense small states possess. In 2015 current Minister for Defense Dr. Ng Eng Hen, stated that total defense is the "exact antagonist" of hybrid warfare.[225] Survival in the world of hybrid war is not just a matter of kinetic conventional capabilities but requires deep integration of the military and civilian sectors to rely on the whole of society. Both the military and public must be competent and committed to defending the nation. With the rise of hybrid warfare, the small, smart power model will become more effective in deterring and defending against hybrid war. Thus, the small, smart power model is not solely a useful framing device for small power but can also serve the use of great powers who face even more vulnerabilities to hybrid war tactics, given they are a larger target.

[225] Ng Eng Hen, "Speech by Dr Ng Eng Hen, Minister for Defence, at Committee of Supply Debate 2015" (MINDEF Singapore, March 5, 2015), https://www.mindef.gov.sg/news-and-events/latest-releases/2015Mar05-Speeches-00648.

Total defense represents the antithesis to total war. All of society's power works towards defending every inch of the nation. Total defense reveals to any adversary that the entirety of the small power's society is resilient and ready to resist any attack. Within this fabric, technology literally connects all of society. It also engages all citizens by encouraging them to produce in the spirit of defending the nation. When total defense is rooted in technology, the state becomes more resilient. For an adversary, the cost of aggression is raised, and the chance of success is decreased. Thus, resilience serves as a deterrent.

References

Alshamy, Yahya, Christopher J Coyne, Nathan P Goodman, and Garrett Wood. “Polycentric Defense, Ukraine Style: Explaining Ukrainian Resilience against Invasion.” *Journal of Public Finance and Public Choice* 39, no. 1 (April 17, 2023): 36–58. https://doi.org/10.1332/251569121x16795569226712.

Andås, Harald Erik. “Emerging technology trends for defence and security.” Norwegian Defense Research Establishment. (2020).

André Beaufre. *An Introduction to Strategy: With Particular Reference to Problems of Defense, Politics, Economics, and Diplomacy in the Nuclear Age* . New York: Praeger, 1965.

Antoniuk, Daryana. “How Ukraine’s Volunteer Hackers Have Created a ‘Coordinated Machine’ around Low-Level Attacks.” The Record. Recorded Future, May 4, 2024. https://therecord.media/ukraine-volunteer-it-army-machine-low-level-attacks.

B. H. Liddell Hart. *Strategy*. New York: Meridian Printing, 1991.

Baldacchino, Godfrey. “Thucydides or Kissinger? A Critical Review of Smaller State Diplomacy.” *The Diplomacies of Small States*, 2009, 21–40. https://doi.org/10.1057/9780230246911_2.

Berman, Ilan I., and Matt Cesare. “Ukraine Reform Monitor No. 1.” American Foreign Policy Council, June 29, 2023. https://www.afpc.org/publications/bulletins/ukraine-reform-monitor/ukraine-reform-monitor-no-1.

Bitzinger, Richard A. “Military-Technological Innovation in Small States: The Cases of Israel and Singapore.” *Journal of Strategic Studies* 44, no. 6 (July 21, 2021): 873–900. https://doi.org/10.1080/01402390.2021.1947252.

Bondar, Kateryna. “How Ukraine Rebuilt Its Military Acquisition System around Commercial Technology.” Center for International Strategic Studies, January 13, 2025. https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.

Cassidy, Robert M. 2002. "Why Great Powers Fight Small Wars Badly." *Military Review* 82 (5) (Sep): 41-53. https://proxy.library.upenn.edu/login?url=https://www.proquest.com/trade-journals/why-great-powers-fight-small-wars-badly/docview/225312626/se-2.

International Institute for Strategic Studies. 1967–1975. *The Military Balance* 1967, 1970, 1975.

London, UK: IISS.

Loo, Bernard Fook Weng. “Explaining Changes in Singapore's Military Doctrines: Material and Ideational Perspectives” in Asia in the New Millennium: APISA First Congress Proceedings, 27-30 November 2003. Edited by Amitav Acharya and Lee Lai To (Singapore: Marshall Cavendish Academic, 2004). 352-375.

———. “Understanding the Military AI Ecosystem of Ukraine.” Center for Strategic and International Studies, November 12, 2024. https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine.

Bonenberger, Adrian. “Ukraine’s Military Pulled Itself out of the Ruins of 2014.” Foreign Policy, May 9, 2022. https://foreignpolicy.com/2022/05/09/ukraine-military-2014-russia-us-training/.

Brik, Tymofii, and Jennifer Brick Murtazashvili. “The Source of Ukraine’s Resilience: How Decentralized Government Brought the Country Together.” Foreign Affairs, June 28, 2022. https://www.foreignaffairs.com/articles/ukraine/2022-06-28/source-ukraines-resilience.

Brown, Shannon A. “Singapore: Civil- Military Fusion and Militarized Civilians.” In *The Routledge Handbook of Civil- Military Relations*, edited by Florina Cristiana Matei, Carolyn Halladay, and Thomas C. Bruneau, 118–30. New York: Routledge, 2021. https://doi.org/10.4324/9781003084228-11.

Bruno, Mark. “‘Uber for Artillery’ - What Is Ukraine’s GIS Arta System? - the Moloch.” The Moloch, August 24, 2022. https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/.

Burke, Joel. “Inside Estonia: How the EU’s E-State Thinks about Defense Tech.” *Emerging Technologies Institute*, September 2024, 1–9.

Cassidy, Robert M. “Why Great Powers Fight Small Wars Badly.” *Military Review* 82, no. 5 (September 2002): 41–53. https://apps.dtic.mil/sti/pdfs/ADA489552.pdf.

Central Intelligence Agency. “Ethnic Groups - the World Factbook: Estonia.” CIA, December 23, 2021. https://www.cia.gov/the-world-factbook/about/archives/2021/countries/estonia.

Chee Hean, Teo. “Speech by Mr Teo Chee Hean, Minister for Defense.” Ministry of Defense Singapore. Presented at the DSTA-DSO Scholarship Award Ceremony, July 8, 2008.

———. “Statement at the 2004 Budget Debate in the Singapore Parliament.” Parliamentary

Debates Official Report - Tenth Parliament. March 15, 2004.

Chin, Kin Wah. "Singapore: Threat Perception and Defence Spending in a City State." In *Defence Spending in Southeast Asia*, edited by Kin Wah Chin, 194–224. Singapore: Institute of Southeast Asian Studies, 1987.

Chong, Alan. "Smart City, Small State: Singapore's Ambitions and Contradictions in Digital Transnational Connectivity." *Journal of International Affairs* 74, no. 1 (2021): 243–60. https://www.jstor.org/stable/27169782.

Choy, Dawen, Ju-Hon Kwek, and Chung Han Lai. *Creating the Capacity to Change: Defence Entrepreneurship for the 21st Century*. Singapore: SAFTI Military Institute, 2003.

Chua, Beng-Huat. *Political Legitimacy and Housing: Singapore's Stakeholder Society*. London: Routledge, 2002.

Cooper, Andrew I, and Timothy M Shaw. "The Diplomacies of Small States at the Start of the Twenty-First Century: How Vulnerable? How Resilient?" In *the Diplomacies of Small States. International Political Economy Series*. London: Palgrave Macmillan, 2009. https://doi.org/10.1057/9780230246911_1.

Cronin, Audrey Kurth. "Open Source Technology and Public-Private Innovation Are the Key to Ukraine's Strategic Resilience." War on the Rocks, August 25, 2023. https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience/.

Cybernetica. "Secure Data Exchange & Interoperability." Cyber.ee, 2025. https://cyber.ee/products/secure-data-exchange/.

Dabila, Antony, and Thibault Fouillet. "What Is Small-State Security Policy?" *Routledge*, September 12, 2023, 118–35. https://doi.org/10.4324/9781003356011-10.

Decker, Audrey. "Ukraine's Cheap Sensors Are Helping Troops Fight off Waves of Russian Drones." Defense One, July 20, 2024. https://www.defenseone.com/defense-systems/2024/07/ukraines-cheap-sensors-are-helping-troops-fight-waves-russian-drones/398204/.

Druziuk, Yaroslav. "A Citizen-like Chatbot Allows Ukrainians to Report to the Government When They Spot Russian Troops — Here's How It Works." Business Insider, April 18, 2022. https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4.

DSO National Laboratories. "Our History." DSO National Laboratories, 2024.

www.dso.org.sg/about/history.

Dudley, William. “Ukraine’s Decentralization Reforms.” *Stiftung Wissenschaft Und Politik (SWP)* 1 (May 2019): 1–34. https://www.swp-berlin.org/publications/products/arbeitspapiere/Ukraine_Decentralization_Dudley.pdf.

Education Estonia. “How It All Began? From Tiger Leap to Digital Society.” Education Estonia, n.d. https://www.educationestonia.org/tiger-leap/.

Ellis, Joseph M. “Estonia’s Innovation Culture: How Did It Happen?” Foreign Policy Research Institute, December 7, 2016. https://www.fpri.org/article/2016/12/estonias-innovation-culture-happen/.

Espinosa, Victor I, and Antonia Pino. “E-Government as a Development Strategy: The Case of Estonia.” *International Journal of Public Administration* 48, no. 2 (February 16, 2024): 1–14. https://doi.org/10.1080/01900692.2024.2316128.

Estonian Parliament . “Eesti Julgeolekupoliitika Alused [Estonian National Security Concept].” *Https://Www.riigiteataja.ee/Aktilisa/0000/1331/4462/13316508.Pdf*, 2010.

Fabian, Sandor. “Professional Irregular Defense Forces: The Other Side of COIN.” 2021. https://apps.dtic.mil/sti/citations/ADA562847.

Fedorov, Mykhailo. “Ukraine’s Vibrant Tech Ecosystem Is a Secret Weapon in the War with Russia.” Atlantic Council, August 17, 2023. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-vibrant-tech-ecosystem-is-a-secret-weapon-in-the-war-with-russia/.

Flanagan, Stephen J., Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin. “Deterring Russian Aggression in the Baltic States through Resilience and Resistance.” *RAND Corporation*, April 15, 2019.

Fontes, Robin, and Jorrit Kamminga. “Ukraine a Living Lab for AI Warfare.” National Defense, March 24, 2023. https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.

Ganesan, Natasha. “Singapore’s Total Fertility Rate Falls to Historic Low of 0.97.” CNA, February 28, 2024. https://www.channelnewsasia.com/singapore/singapore-total-fertility-rate-population-parents-children-4155616.

Ganor, Michael, and Yuli Ben-Lavy. “Community Resilience: Lessons Derived from Gilo under Fire.” *Journal of Jewish Communal Service* 79, no. 2/3 (2003): 105–8.

https://coilink.org/20.500.12592/383f6s.

Glebov, Sergii, and Denys Kuzmin. “On the Way to Ukraine’s Total Defence System.” In *European Total Defence: Past, Present, and Future*, edited by Gjermund Forfang Rongved. London: Routledge, 2025. https://doi.org/10.4324/9781003497370-2.

Goble, Paul. “Experts: Estonia Has Successfully Integrated Nearly 90% of Its Ethnic Russians.” Estonian World, March 1, 2018. https://estonianworld.com/security/experts-estonia-successfully-integrated-nearly-90-ethnic-russians/.

Goble, Paul A. “Last Lenin Statue in Ukraine Falls - Euromaidan Press.” Euromaidan Press, January 31, 2021. https://euromaidanpress.com/2021/01/31/last-lenin-statue-in-ukraine-falls/.

Gorchinskaya, Katya. “Ukroboronprom Director Says Weapons Shipments to Russia Stopped Three Weeks Ago.” Kyiv Post, April 15, 2014. https://www.kyivpost.com/post/10033.

Grzegorzewski, Mark, Margaret Smith, and Barnett Koven. “Civil Cyber Defense – a New Model for Cyber Civic Engagement.” *The Cyber Defense Review* 8, no. 3 (2023): 51–66. https://doi.org/10.2307/48755361.

Hambling, David. “Only the Brave: How Ukrainians Can Take on Russian Tanks with Molotov Cocktails.” Forbes, March 2, 2022. https://www.forbes.com/sites/davidhambling/2022/03/02/only-the-brave-how-ukrainians-can-take-on-tanks-with-molotov-cocktails/.

Hashim, Ahmed S. “Security & Defense in Small States: Qatar, the UAE and Singapore.” *Middle East Policy* 27, no. 3 (September 2020): 30–45. https://doi.org/10.1111/mepo.12511.

Hen, Ng Eng. “Speech by Dr Ng Eng Hen, Minister for Defence, at Committee of Supply Debate 2015.” MINDEF Singapore, March 5, 2015. https://www.mindef.gov.sg/news-and-events/latest-releases/2015Mar05-Speeches-00648.

Henrikson, Alan K. “A Coming ‘Magnesian’ Age? Small States, the Global System, and the International Community.” *Geopolitics* 6, no. 3 (December 2001): 49–86. https://doi.org/10.1080/14650040108407729.

Holtom, Paul. “Ukrainian Arms Supplies to Sub-Saharan Africa.” *Stockholm International Peace Research Institute*, February 2011, 1–16. https://www.sipri.org/sites/default/files/files/misc/SIPRIBP1102.pdf.

Huxley, Tim. *Defending the Lion City: The Armed Forces of Singapore*. St. Leonards Australia:

Allen & Unwin, 2000.

———. “Singapore and Military Transformation.” In *The RMA for Small States: Theory and Application*. Singapore, 2004.

Ingebritsen, Christine, Iver Neumann, Sieglinde Gstohl, and Jessica Beyer. *Small States in International Relations*. *JSTOR*. University of Washington Press, 2006. https://www.jstor.org/stable/j.ctvcwnw88.

Ingram, George, and Priya Vora. “Ukraine: Digital Resilience in a Time of War.” Brookings Institute, January 30, 2024. https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/.

Invest Estonia. “Estonia Leads Europe in Startups, Unicorns and Investments per Capita.” Invest in Estonia, December 2022. https://investinestonia.com/estonia-leads-europe-in-startups-unicorns-and-investments-per-capita/.

Ispas , Irina. “Principle of Military Innovation as an Upgrade to the Army Concept: Differences, Similarities and Lessons. A Case Study of Israel and Estonia.” 2019.

Jasper, Scott. “Resilience against Hybrid Threats: Empowered by Emerging Technologies: A Study Based on Russian Invasion of Ukraine.” In *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies*, edited by Panos M. Pardalos and My T. Thai, 209–26. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-39542-0_10.

Jermalavičius, Tomas, and Martin Hurt. “Defence Innovation: New Models and Procurement Implications – the Estonian Case.” *Armament Industry European Research Group, French Institute for International and Strategic Affairs (IRIS)*, September 2021, 1–23.

Jermalavičius, Tomas, and Merle Parmak. “Towards a Resilient Society, or Why Estonia Does Not Need ’Psychological Defence’.” *International Centre for Defence Studies*, September 2012, 1–19. https://eprints.hud.ac.uk/id/eprint/21718/1/ParmakTowards.pdf.

Jervis, Robert. “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (January 1978): 167–214. https://doi.org/10.2307/2009958.

Jordan, Józef Witold. “Evolution of the Concept of Total Defence in the Baltic States.” *Rozprawy Społeczne* 18, no. 1 (July 11, 2024): 315–44. https://doi.org/10.29316/rs/188761.

Kaljurand, Riina. “Security Challenges of a Small State: The Case of Estonia.” In *Defense and*

Security for the Small: Perspectives from the Baltic States, 2013.

Keohane, Robert O. "Lilliputians' Dilemmas: Small States in International Politics." *International Organization* 23, no. 2 (1969): 291–310. https://www.jstor.org/stable/2706027.

Khoo, Jimmy. "Keynote Address by Future Systems Architect, BG Jimmy Khoo at C4I Asia Conference." Ministry of Defense Singapore. Presented at the C4I Asia Conference, February 23, 2004.

Kissinger, Henry A. "The Vietnam Negotiations." *Survival* 11, no. 2 (February 1969): 38–50. https://doi.org/10.1080/00396336908440951.

Kudelia, Serhiy. "The Ukrainian State under Russian Aggression." *Current History* 121, no. 837 (October 1, 2022): 251–57. https://doi.org/10.1525/curh.2022.121.837.251.

Kudlenko, Anastasiia. "Roots of Ukrainian Resilience and the Agency of Ukrainian Society before and after Russia's Full-Scale Invasion." *Contemporary Security Policy* 44, no. 4 (September 20, 2023): 1–17. https://doi.org/10.1080/13523260.2023.2258620.

Kuzmuk, Kateryna , and Lorenzo Scarazzato. "The Transformation of Ukraine's Arms Industry amid War with Russia." SIPRI, February 21, 2025. https://www.sipri.org/commentary/topical-backgrounder/2025/transformation-ukraines-arms-industry-amid-war-russia.

Kyiv School of Economics. "Report on Damages to Infrastructure from the Destruction Caused by Russia's Military Aggression against Ukraine as of January 2024," April 2024. https://kse.ua/wp-content/uploads/2024/05/Eng_01.01.24_Damages_Report.pdf.

Lawrence, Tony. "Estonia: Size Matters." *PRISM* 10, no. 2 (March 10, 2023): 19–37.

Lee Kuan Yew. *From Third World to First: The Singapore: 1965-2000*. Singapore: Times Publishing Group, 2015.

Lee, Edwin. *Singapore : The Unexpected Nation*. Singapore: Institute Of Southeast Asian Studies, 2008.

Levy, Jack S. *War in the Modern Great Power System: 1495-1975*. University Press of Kentucky, 1983. https://doi.org/10.2307/j.ctt130jjmm.

Liebermann, Oren. "How Ukraine Is Using Resistance Warfare Developed by the US to Fight Back against Russia." CNN, August 27, 2022. https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

Lindegaard, Lily Salloum, and Neil Anthony Webster. “Supporting Political Stability by Strengthening Local Government: Decentralisation in Ukraine.” *Danish Institute for Interational Studies* 2018, no. 7 (May 28, 2018): 1–96. https://pure.diis.dk/ws/files/2543996/DIIS_Report_07_Ukraine_WEB.pdf.

Loo, Bernard Fook Weng. “The Management of Military Change: The Case of the Singapore Armed Forces.” In *Security, Strategy and Military Change in the 21st Century*, edited by Jo Inge Bekkevold, Ian Bowers, and Michael Raska, 70–88. Routledge, 2015.

Lopatin, Mykhaylo. “Bind Ukraine’s Military-Technology Revolution to Rapid Capability Development.” War on the Rocks, January 23, 2024. https://warontherocks.com/2024/01/bind-ukraines-military-technology-revolution-to-rapid-capability-development/.

Lumack, Robert. “Defence and Military Reform in Ukraine 2014-2022.” 2025. https://doi.org/10.20381/ruor-30833.

Mamediieva, Gulsanna, and Donald P Moynihan. “Digital Resilience in Wartime: The Case of Ukraine.” *Public Administration Review* 83, no. 6 (October 22, 2023): 1512–16. https://doi.org/10.1111/puar.13742.

Manish Jung Pulami. “Analysing Revitalised Security Industry: The Tech-Powered Transformation for Small States.” *Unity Journal* 5, no. 1 (March 25, 2024): 301–15. https://doi.org/10.3126/unityj.v5i1.63195.

Manolache, Ionela Cătălina. “Leveraging Emerging and Disruptive Technologies to Streamline the Deployment Process and Enhance Force Protection in Current and Future Operating Environment.” *Strategic Impact* 91, no. 2 (October 9, 2024): 97–111. https://doi.org/10.53477/1842-9904-24-11.

Matthews, Ron, and Fitriani Bintang Timur. “Singapore’s ’Total Defence’ Strategy.” *Defence and Peace Economics* 35, no. 5 (March 9, 2023): 1–21. https://doi.org/10.1080/10242694.2023.2187924.

Matthews, Ron, and Nellie Zhang Yan. “Small Country ‘Total Defence’: A Case Study of Singapore.” *Defence Studies* 7, no. 3 (September 2007): 376–95. https://doi.org/10.1080/14702430701559289.

McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” *BBC News*, April 27, 2017. https://www.bbc.com/news/39655415.

McLees, Alexandra, and Eugene Rumer. “Saving Ukraine’s Defense Industry.” Carnegie Endowment for International Peace, July 30, 2014. https://carnegieendowment.org/research/2014/07/saving-ukraines-defense-industry?lang=en.

Mearsheimer, John. *The Tragedy of Great Power Politics*. New York: W.W. Norton & Company, 2014.

MilMag. “Estonia’s Defense Industry – Small but InnovativeThis Text Comes from MILMAG Military Magazine. Read More On:https://Milmag.pl/En/Estonias-Defense-Industry-Small-But-Innovative/,” December 19, 2024. https://milmag.pl/en/estonias-defense-industry-small-but-innovative/.

Ministry of Defense Singapore. “Defence Science & Technology.” MINDEF, 2024. https://www.mindef.gov.sg/defence-matters/defence-topic/defence-science-technology.

Morrison, Charles Edward, and Astri Suhrke. *Strategies of Survival: The Foreign Policy Dilemmas of Smaller Asian States*. Australia: University of Queensland Press, 1978.

Nam, Nicholas. “Reform of Asset and Interest Disclosure in Ukraine.” *World Bank Group*, January 16, 2021, 232–37. https://thedocs.worldbank.org/en/doc/457791611679267058-0090022021/original/ReformofAssetandInterestDisclosureinUkraine.pdf.

NATO. “Deterrence and Defence.” NATO, December 10, 2023. https://www.nato.int/cps/en/natohq/topics_133127.htm.

NATO Cooperative Cyber Defence Centre of Excellence. “World’s Largest Cyber Defense Exercise Locked Shields Brings Together over 3000 Participants.” NATO CCDCOE, April 18, 2023. https://ccdcoe.org/news/2023/6016/.

NATO Science & Technology Organization. “Science & Technology Trends 2023-2043,” March 2023. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

Ng, Pak Shun. *From “Poisonous Shrimp” to “Porcupine”: An Analysis of Singapore’s Defence Posture Change in the Early 1980s*. Canberra: National Library of Australia, Strategic and Defence Studies Centre, 2005.

O’Loughlin, John, and Gerard Toal. “Does War Change Geopolitical Attitudes? A Comparative Analysis of 2014 Surveys in Southeast Ukraine.” *Problems of Post-Communism* 67, no. 3 (November 15, 2019): 303–18. https://doi.org/10.1080/10758216.2019.1672565.

Oleinikova, Olga. “Decentralization Reform: An Effective Vehicle for Modernization and

Democratization in Ukraine?" In *Decentralization, Regional Diversity, and Conflict*, edited by Hanna Shelest and Maryna Rabinovych, 311–38. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-41765-9_11.

Oprişor, Ion. "The Impact of Emerging and Disruptive Technologies on Security." *Land Forces Academy Review* 26, no. 4 (December 1, 2021): 261–68. https://doi.org/10.2478/raft-2021-0033.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, 2008.

Paul, T.V. *Asymmetric Conflicts: War Initiation by Weaker Powers*. Vol. 33. Cambridge University Press, 1994.

Pevkur, Hanno. Interview with the Honorable Hanno Pevkur: Minister of Defense of Estonia. Interview by Michael Miklaucic. *PRISM (National Defense University Press)*, June 2, 2023. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3512177/interview-with-the-honorable-hanno-pevkur-minister-of-defense-of-estonia/.

Pham, P. L. *Ending "East of Suez."* Oxford: Oxford Historical Monographs, 2010. https://doi.org/10.1093/acprof:oso/9780199580361.001.0001.

Putrenko, Viktor, and Nataliia Pashynska. "Military Situation Awareness: Ukrainian Experience." *Applied Cybersecurity & Internet Governance* 3, no. 1 (July 17, 2024): 122–46. https://doi.org/10.60097/acig/190341.

Raska, Michael. *Military Innovation in Small States*. Routledge, 2015.

———. "The Contours of Singapore's Defence Planning: Rethinking Deterrence, Defence Diplomacy, and Resilience." In *Defence Planning for Small and Middle Powers*, 45–74. Taylor & Francis, 2024.

Raud, Mikk. "Hedgehog Meets Dolphin: Can Estonia Adopt Singapore's Secret Weapon—Defence Innovation?" International Centre for Defence and Security (ICDS), 2018. JSTOR. https://doi.org/10.2307/resrep54308.

Redick, James, and Glenn Jones. *The Need for an Integrated Strategy: Denial, Deterrence, and Relentless Resilience*. North American Aerospace Defense Command, 2021.

Republic of Estonia: Government Office. "The Government Approved a Comprehensive Approach towards Development Civil Protection," 2018.

https://www.valitsus.ee/en/news/government-%20approved-comprehensive-approach-towards-developing-civil-protection.

Rothstein, Robert L. *Alliances and Small Powers*. New York: Columbia University Press, 1968.

Rotolo, Daniele, Diana Hicks, and Ben R. Martin. "What Is an Emerging Technology?" *Research Policy* 44, no. 10 (December 2015). https://doi.org/10.1016/j.respol.2015.06.006.

Sarkissian, Armen. *The Small States Club: How Small States Can Save the World*. London: C. Hurst & Co., 2024.

Schmidt, Eric, and Helene Cooper. "Pentagon Chief Speaks to Russian Counterpart after Drone Incident." New York Times, March 15, 2023. https://www.nytimes.com/live/2023/03/15/world/russia-ukraine-news.

Shelest, Hanna. "Defend. Resist. Repeat: Ukraine's Lessons for European Defence." European Council on Foreign Relations, November 9, 2022. https://ecfr.eu/publication/defend-resist-repeat-ukraines-lessons-for-european-defence/.

Shimooka, Richard. "Towards a Better Integrated, Better Equipped Ukraine: Richard Shimooka." Macdonald-Laurier Institute, February 16, 2024. https://macdonaldlaurier.ca/towards-a-better-integrated-better-equipped-ukraine/.

Singapore Defence Science and Technology Agency. "Imagining What's Next." DSTA, July 4, 2025. https://www.dsta.gov.sg/whats-on/spotlight/imagining-what.

Singapore Ministry of Defence. "News Release: Factsheet - about Total Defence," 2004. https://www.nas.gov.sg/archivesonline/data/pdfdoc/MINDEF_20040207001_2/MINDEF_20040207003.pdf.

———. "Total Defence," 2024. https://www.mindef.gov.sg/defence-matters/defence-topic/total-defence.

Singh, Bilveer. *Arming the Singapore Armed Forces (SAF)): Trends and Implications*. Canberra: Strategic and Defense Studies Center, ANU, 2003.

Sipahi, Esra Banu, and Zabihullah Say. "The World's First 'Smart Nation' Vision: The Case of Singapore." *Smart Cities and Regional Development Journal* 8, no. 1 (2024): 41–58.

Spencer, John, and Liam Collins. "How Volunteers Can Help Defeat Great Powers." Military Times, July 5, 2022. https://www.militarytimes.com/opinion/commentary/2022/07/05/how-volunteers-can-

defeat-great-powers/.

Starodubtsev, Olexandr. *YOUkraine. Because ProZorro.* World Bank, 2015. https://thedocs.worldbank.org/en/doc/828301490813177880-0310022017/original/UseofeGPforopenDataOlexandr.pdf.

Stocholm International Peace Reseach Institute. "The SIPRI Top 100 Arms-Producing and Military Services Companies in the World, 2023." SIPRI, 2023. https://www.sipri.org/visualizations/2024/sipri-top-100-arms-producing-and-military-services-companies-world-2023.

Szymański, Piotr. *New Ideas for Total Defense: Comprehensive Security in Finland and Estonia*. Warsaw, Poland: Centre for Eastern Studies, 2020.

Talfryn, Owain Llŷr. "Learning from Estonia: How a Young Nation Became a Leader in Digital Living." Stellar Capacity, December 23, 2021. https://www.stellarcapacity.com/post/learning-from-estonia-how-a-young-nation-became-a-leader-in-digital-living.

Tan, Andrew. "Domestic Determinants of Singapore's Security Policy." *Asia-Pacific Center for Security Studies*, 2001.

Tkachuk, Anatoliy. "Decentralization, Progress, Risks and Role of the Ukrainian Parliament - Інститут громадянського суспільства." Dzerkalo Tyzhnia, January 13, 2017. https://www.csi.org.ua/news/decentralization-progress-risks-role-ukrainian-parliament/.

Toulas, Bill. "Ukraine Says Its 'IT Army' Has Taken down Key Russian Sites." BleepingComputer, February 28, 2022. https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/.

Veebel, Viljar, Illimar Ploom, Liia Vihmand, and Krzystof Zaleski. "Territorial Defence, Comprehensive Defence and Total Defence: Meanings and Differences in the Estonian Defence Force." *Journal on Baltic Security* 6, no. 2 (December 8, 2020). https://doi.org/10.2478/jobs-2020-0007.

Verkhovna Rada. "Law of Ukraine on the Basis of National Resistance." Verkhovna Rada, 2021. https://zakon.rada.gov.ua/laws/show/1702-20#Text.

Vincic, Neven. "The Future of Warfare: Security Implications of Emerging and Disruptive Technologies (EDTs)." NATO Association of Canada, May 12, 2021.

https://natoassociation.ca/the-future-of-warfare-security-implications-of-emerging-and-disruptive-technologies-edts/.

Vital, David. *The Inequality of States*. Oxford: Clarendon Press, 1967.

Vlasiuk, Volodymyr, Luke Cooper, and Brian Milakovsky. "A State-Led War Economy in an Open Market Investigating State-Market Relations in Ukraine 2021-2023." *LSE Conflict and Civicness Research Group*, June 4, 2024. https://peacerep.org/wp-content/uploads/2024/06/A-state-led-war-economy-in-an-open-market-DIGITAL.pdf.

Vosman, Andres, and Magnus Petersson. *European Defence Planning and the Ukrainian Crisis: Two Contrasting Views*. Institut Français des Relations Internationales (IFRI)., 2015.

Waltz, Kenneth. *Theory of International Politics*. 1st ed. New York: Random House, 1979.

Wang, Ning. "Singapore's Experience and Enlightenment of Building a 'Smart Nation.'" Edited by K.H.M. Mansur and Y. Fu. *E3S Web of Conferences* 251 (2021). https://doi.org/10.1051/e3sconf/202125101069.

Wezeman, Siemon T., and Sam Perlo-Freeman. "The Ukraine Conflict and Its Implications: III. The Impact of the Crisis in Ukraine on Arms Transfers." In *SIPRI Yearbook 2015 : Armaments, Disarmament and International Security*, 86–98. World Armaments And Disarmament Oxford: Oxford University Press, 2015.

Wong, Cara. "Budget Debate: Contact Tracing Process Shortened with Almost 90% of S'pore Residents Using TraceTogether." The Straits Times, February 26, 2021. https://www.straitstimes.com/singapore/politics/almost-90-per-cent-of-residents-on-tracetogether-programme.

Yermolenko, Volodymyr. "Ukraine's Resilience and Why It Continues to Fight." Chatham House, February 8, 2023. https://www.chathamhouse.org/2023/02/ukraines-resilience-and-why-it-continues-fight.

Yew, Lee Kuan. "The Fundamentals of Singapore's Foreign Policy: Then & Now." Presented at the S. Rajaratnam Lecture at MFA Diplomatic Academy, May 9, 2009. https://www.pmo.gov.sg/Newsroom/speech-mr-lee-kuan-yew-minister-mentor-s-rajaratnam-lecture-09-april-2009-530-pm-shangri.

Zelenskyy, Volodymyr. "Decree of the President of Ukraine No.121/2021." Preside of Ukraine, 2021. https://www.president.gov.ua/documents/1212021-37661.