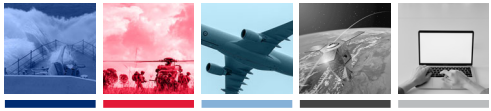
ADF Land Domain Publication



Land Domain Publication - Note

LNote 7.2.4 Olvanan Espionage Framework and Tactics

Issued by authority of the Chief of Army.

Publication release approved on 15 July 2025 in accordance with the Army Standing Instruction (Knowledge Management) Part 2 – *Management and Governance of ADF Land Domain Publications*.

EDITION 1

LNote 7.2.4 *Olvanan Espionage Framework and Tactics*

Edition 1, 2025

ISBN: 978-1-922908-56-8

Sponsor: Chief of Army

Accountable Officer: Army G7

Release Authority: Staff Officer Grade One Land Domain Publications

Content Adviser: Commander Army Battle Lab

1. https://www.legislation.gov.au/Series/C1968A00063
2. https://www.legislation.gov.au/Series/C2004A04868
3. https://www.legislation.gov.au/Series/C2004A03712
4. http://drnet/AssociateSecretary/security/policy/Pages/dspf.aspx

Preface

1. ADF Land Domain Publications (LPubs) describe the fundamental principles that guide land forces actions, and provide the common frame of reference on how the Army achieves its mission. LPubs are the basis of the Army's training system based on time-tested, proven principles of war, combined with the critical analysis of contemporary lessons. LPubs have been shaped since 1901 by Army's proud history and culture, while being constantly adapted as required, thereby representing the sum of the Army's collective historical knowledge, presented into objective guides for action. In essence LPubs explain and guide *'who we are', 'what we do' and 'how we do it'*.

2. ADF doctrine provides the framework that guides thinking but does not dictate what to do. While doctrine publications are written in a non-prescriptive style that allows latitude in interpretation and flexibility in application, they are specific enough to provide informed guidance. Doctrine is about fighting power and the integration of its three components: intellectual, moral and physical, applied through mission command and our manoeuvrist approach to warfighting.

3. Land procedural publications provide the authorised procedural and technical knowledge required for land forces to achieve their mission. Unlike doctrine, procedural publications convey information covering a range of activities based on best possible practice, in clear detailed steps that, depending on the publication, describe and/or prescribe how to perform specific tasks and drills. Whilst the majority of procedural publications are descriptive in nature, the decision not to follow the guidance contained in the publications should be justifiable. Land procedural publications are aligned and subordinate to ADF doctrine.

4. Land procedural publications include a number of publications that prescribe the procedures for the safe conduct of a range of tasks and activities required for delivering a range of lethal warfighting capabilities. Procedural publications which are safety in nature are written with an expectation of compliance, and therefore do not attempt to prescribe every 'do' and 'don't'. A number of land procedural publications are classified as Landworthiness Regulations

in accordance with *Defence Landworthiness Management System Manual*. **LPubs constitute a lawful general order when written in mandatory terms and apply to all personnel**.

5. **Land Domain Publication - Note (LNote)** is a provisional publication valid for no more than 24 months from its release until it is cancelled, released as an enduring LPub or absorbed into an existing LPub. LNote can be released:

a. as an addendum to an existing land publication

b. to provide additional information of significance in a timely manner to address an emerging issue, an identified lesson, or to satisfy a major/critical knowledge gap

c. as an unscheduled/short notice new publication, published in response to changing strategic guidance, introduction of new capabilities, emerging threats or opportunities.

Aim

6. LNote 7.2.4 *Olvanan Espionage Framework and Tactics* aims to provide an in-depth understanding on how the training adversary will conduct espionage operations to support its objectives.

Land publication L-Library

7. The ADF Land Power Library (L-Library) is the single access point, and digital catalogue for Army's authorised land power artefacts, supporting resources, including other related publications. In addition to accessing all current and historical publications, the L-Library contains links to ADF doctrine, and other ADF domain publications, as well as approved international partner publications. The L-Library is accessible via ADF Land Power Library and Army Knowledge Online.

8. Additional printed copies of Land Publications may be ordered using the Defence Print Ordering Portal which can be accessed via this link: https://printportal/overview.web.

Security

9. This publication contains Australian Defence information for the purposes of the *Crimes Act 1914* (Commonwealth) (the Act) and carries a protective marking in compliance with the Defence Security Principles Framework (DSPF). The publication and the information contained therein must be treated and secured in accordance with that protective marking. All Defence information, whether classified or not, is protected from unauthorised disclosure under the Act and may only be released in accordance with the procedures stipulated within the DSPF. Any requests for release of this publication or part thereof must be forwarded to Land Domain Publications. The publication must not be released to non-Defence agencies or persons without written authority from Land Domain Publications.

This page intentionally blank

Amendment record

1. Amendments to this Land Domain Publication are issued on the authority of the Chief of Army pursuant to Army Standing Instruction (Knowledge Management) Part 2 – *Management and Governance of ADF Land Domain Publications*.

Number	Date of amendment	Authorised by
1.		
2.		
3.		
4.		
5.		

2. All superseded amendment record pages should be retained at the rear of the publication for audit purposes.

3. Proposals to amend this publication may be emailed to: armybattlelab.landdomainpublications@defence.gov.au.

This page intentionally blank

Contents

List of figures

List of tables

Chapter 1

History of Olvanan espionage

Section 1-1. The Imperial era: Dawn of espionage

1.1 The origins of Olvanan intelligence trace back to the 5th century BC, during a fragmented period of warring states. A key figure in this era, Moon Dao, authored The Essence of Strategy, a military treatise emphasising the vital role of spies in warfare. His teachings shaped Olvanan rulers' approach to governance, emphasising that intelligence, rather than sheer military strength, was the key to victory.

1.2 With the institutionalisation of espionage, rulers formalised spy networks, training agents in disguise, cryptography and psychological manipulation.

Dynastic intelligence networks

1.3 The Xao dynasty (221–206 BC) established the Eyes and Ears of the Emperor, a vast network of informants and spies.

1.4 The Lim dynasty (206 BC–220 AD) advanced encryption techniques and early psychological warfare, refining intelligence into a structured state apparatus.

Golden age of espionage

1.5 The Jinrong (618–907 AD) and Heming (960–1279 AD) dynasties expanded espionage through the Bureau of Shadow Strategies, embedding agents across the empire and beyond.

1.6 By the end of the imperial era, intelligence had become a cornerstone of Olvana's military and political strategy, ensuring both internal stability and external dominance.

Section 1-2. The Republican era: Intelligence as a tool of political control

1.7 Following the fall of the monarchy, Olvana entered a period of national instability. Intelligence efforts during this era were characterised by two competing factions:

a. The Nationalist Government – Developed counterintelligence operations to suppress opposition and secure state power.

b. The Olvanan Communist Party (OCP) – Created a grassroots intelligence network to infiltrate government structures and coordinate revolutionary activities.

1.8 The struggle between these factions evolved into a full-scale intelligence war, with both sides using propaganda, infiltration, and counter-espionage tactics. This period solidified the role of espionage as a central instrument of power.

Early People's Republic: Intelligence centralisation and Cold War expansion

1.9 With the establishment of the People's Republic of Olvana (PRO) in 1951, intelligence operations became centralised under the newly formed Ministry of National Security (MNS) and the military's Olvanan People's Army (OPA) intelligence units. These agencies played a dual role:

a. *Domestic surveillance.* The MNS focused on eliminating internal dissent, monitoring political activities, and suppressing counter-revolutionary movements.

b. *International espionage.* Olvana aligned its intelligence strategy with Cold War dynamics, engaging in:

   (1) Military and technological espionage to counter Western advances.

   (2) Support for revolutionary movements to expand ideological influence.

1.10 This period marked the expansion of intelligence as a key instrument of statecraft, laying the foundation for Olvana's modern espionage strategies.

Section 1-3. Contemporary era: Cyber and global espionage

1.11 With the advent of digital technologies and economic liberalisation, Olvana shifted towards cyber-espionage, industrial intelligence, and global surveillance. Key developments include:

a. Cyber and technological espionage:

   (1) Development of state-backed cyber units to infiltrate foreign governments, defence firms, and corporations.

   (2) Use of artificial intelligence to automate intelligence collection and analysis.

b. State Owned Enterprises (SOEs) as espionage fronts:

   (1) Leveraging international business partnerships to gain access to sensitive technologies.

   (2) Recruiting insiders within multinational corporations to extract trade secrets.

c. Soft power and influence operations:

   (1) Expansion of the Global Outreach and Coordination Office (GOCO) to control foreign narratives and manipulate political landscapes.

1.12 Modern Olvanan espionage extends beyond traditional intelligence gathering, encompassing cyber warfare, economic sabotage, and geopolitical influence, making it a formidable force in international affairs.

1.13 Olvana's espionage operations have evolved from ancient spy networks to a highly sophisticated intelligence apparatus capable of cyber infiltration, industrial espionage, and geopolitical manipulation. This evolution reflects the state's long-standing reliance on intelligence as a strategic tool for national security, economic

advancement, and global dominance. Understanding this historical trajectory provides critical insights into Olvana's current and future intelligence strategies.

1.14 A detailed history of Olvanan espionage can be found in Annex 1A.

Annex:

1A Detailed history of Olvanan espionage

Annex 1A

Detailed history of Olvanan espionage

The golden age of espionage: The Jinrong and Heming dynasties

1. The Jinrong (AD 618–907) and Heming (AD 960–1279) dynasties represent the golden age of espionage in Imperial Olvana. During these periods, the state developed a highly organised bureaucratic system dedicated to intelligence gathering. The Jinrong dynasty established the ‘Bureau of Shadow Strategies,’ which oversaw a network of undercover agents throughout the empire and beyond.

2. These agents, often posing as merchants, monks, or travellers, played key roles in the empire’s expansion and the maintenance of its power. They were tasked with mapping uncharted territories, establishing trade routes, and negotiating alliances. The Heming dynasty continued these practices, with an added focus on technological innovation. The creation of the ‘Silent Messengers’ — messages encoded in seemingly innocuous objects — was a testament to the ingenuity of Olvanan intelligence.

The height of imperial espionage: The Guanghai and Xingji dynasties

3. The Guanghai (AD 1368–1644) and Xingji (AD 1644–1912) dynasties marked the peak of Imperial Olvana’s intelligence operations. The Guanghai dynasty’s ‘Imperial Directive for the Unseen War’ formalised espionage as a state function, recognising its agents as key to the empire’s survival and prosperity. The Xingji dynasty, however, took these practices to unprecedented levels, establishing the ‘Great Web of Shadows’ — a network that extended across continents, leveraging the growing global trade networks to gather intelligence on European powers, neighbouring Asian states, and emerging entities in the Americas.

4. The Xingji dynasty's intelligence apparatus was a marvel of complexity and efficiency. It comprised specialised divisions for cryptography, counterintelligence, and foreign espionage. The use of secret societies and guilds as fronts for espionage activities demonstrated the dynasty's sophisticated understanding of non-traditional warfare. The 'Invisible Flames' — a group of agents' adept in sabotage and psychological operations — were a testament to the Xingji dynasty's innovative approach to intelligence.

The Republican era: A nation in turmoil

5. The fall of the Xingji dynasty in 1912 marked the end of imperial rule and ushered in the Republican era, a period characterised by political fragmentation, civil unrest, and the reformation of intelligence practices in the face of modern challenges. This tumultuous era saw the rise of the Republic of Olvana, a nation striving to find its identity amidst internal strife and external pressures.

The dawn of republican intelligence

6. In the early days of the Republic, Olvana was a concoction of conflicting interests, with various warlords, emerging political parties, and foreign powers vying for influence. The fragmentation of the once unified imperial intelligence system gave rise to a decentralised network of operatives aligned with different factions. It was during this time that the Olvanan Hindu Nationalists supported by several smaller nationalist groups and the Olvanan Communist Party (OCP) began to develop their intelligence capabilities, laying the groundwork for a new era of espionage.

7. The Nationalist government, seeking to consolidate power and unify the nation under its banner, established the Bureau of Investigation and Statistics. This agency was tasked with counter-espionage, internal security, and the collection of political intelligence. It employed a range of tactics, from surveillance to the infiltration of rival factions and foreign embassies. The Bureau played a crucial role in the Nationalists' attempts to stabilise the country and assert control over its disparate regions.

The Olvanan Communist Party's intelligence network

8. Parallel to the Nationalist efforts, the OCP recognised early on the importance of intelligence in its struggle for power. Operating under the radar, the OCP's intelligence network was adept at guerrilla tactics, propaganda dissemination, and the orchestration of strikes and uprisings. Its operatives, often working in the shadows, were instrumental in gathering information on Nationalist troop movements, securing support from rural populations, and forging alliances with other anti-Nationalist forces.

9. The OCP's intelligence operations were characterised by their grassroots nature, leveraging the party's deep connections within communities to elicit information and coordinate activities against the Nationalist regime. This approach not only enabled the OCP to survive crackdowns but also to build a base of support that would eventually contribute to its ascension to power.

Intelligence warfare and the struggle for Olvana

10. The Republican era was a crucible in which the modern intelligence apparatus of Olvana was forged. Both the Nationalists and the OCP engaged in a shadow war, where information was as crucial as firepower. Espionage and counter-espionage activities permeated every aspect of the struggle for control of the country, from the battlefields to the political arenas.

11. The era was marked by significant espionage operations, including the interception of communications, the use of propaganda to sway public opinion, and the deployment of spies to infiltrate the highest levels of opposing factions. These intelligence activities were not just ancillary to the military campaigns; they were central to the strategies employed by both sides in their quest for dominance.

Legacy of the Republican era

12. The Republican era's legacy in terms of intelligence was the recognition of its vital role in modern statecraft and warfare. The period's challenges necessitated innovations in intelligence tactics and techniques, many of which would be carried forward into the People's Republic era. Moreover, the era underscored the importance

of intelligence in not only shaping military and political outcomes but also in forging a national identity amidst the chaos of transition.

13. Donovia's Communist government provided material support and advisors to the Olvanan Communists, enabling them to intensify their campaign, and take control of all of Olvana by using a divide and conquer strategy and mobilising the rural population.

14. As the Republican era gave way to the establishment of the PRO on 01 November 1951, the lessons learned, and the capabilities developed during this period would prove instrumental in shaping the future of Olvanan intelligence. The foundation laid during these tumultuous years would enable the OCP to centralise and expand its intelligence operations, marking the beginning of a new chapter in Olvana's history.

Early People's Republic of Olvana: The consolidation of power through intelligence

15. The establishment of the PRO marked a monumental shift in the nation's governance and strategic direction. Central to this transformation was the reorganisation and centralisation of intelligence operations under the guidance of the Olvanan Communist Party (OCP), which sought to secure its emerging regime against internal dissent and external threats. This period, stretching from 1951 to the late 1970s, witnessed the instrumental use of intelligence in consolidating power and projecting Olvana's influence on the global stage.

Centralisation of intelligence operations

16. Upon coming to power, the OCP quickly moved to centralise intelligence operations, recognising the critical role they played in maintaining state security and advancing the party's objectives. The MNS was established as the primary entity responsible for both domestic surveillance and foreign espionage. The OPA also maintained its own intelligence units, focusing on military intelligence and counterintelligence efforts to safeguard national defence under the framework of Supreme High Command (SHC).

17. The MNS and OPA intelligence units work in tandem, though with distinct mandates. The MNS is tasked with rooting out

counter-revolutionary elements, gathering political intelligence, and overseeing espionage activities abroad. The OPA, meanwhile, focused on acquiring military intelligence, assessing foreign military capabilities, and supporting the OCP's strategic military objectives.

The role of intelligence in domestic surveillance

18. Domestic surveillance was intensified during the early years of the PRO, aimed at consolidating the OCP's control over the populace and preventing any form of dissent that could destabilise the regime. The MNS deployed a vast network of informants across the country, infiltrating every level of society from the rural communes to the urban centres. This network was instrumental in identifying and neutralising potential threats to the state, including real and perceived opponents of the regime.

19. The use of propaganda, psychological operations, and re-education programs were also key components of the OCP's strategy to maintain its grip on power. Intelligence agencies played a crucial role in shaping public opinion and ensuring the party's ideology was deeply ingrained in the social fabric of Olvana.

Foreign espionage and the Cold War

20. The geopolitical tensions of the Cold War provided both challenges and opportunities for the PRO. The OCP sought to position Olvana as a leader of the global communist movement, extending its influence through support for revolutionary groups and governments in Asia, Africa, and Latin America. The MNS and OPA intelligence units conducted operations to gather critical intelligence on Western powers, particularly the United States and its allies, as well as monitoring the activities of the rival Soviet bloc.

21. Espionage activities during this period included the acquisition of technological and military secrets, infiltration of foreign governments and institutions, and the execution of covert operations to support allied movements. The intelligence gleaned from these operations was vital in informing Olvana's foreign policy and military strategies, enabling the country to navigate the complex dynamics of the Cold War.

The impact of intelligence on Olvana's global position

22. The early PRO era demonstrated the strategic value of intelligence in achieving national objectives. The OCP's ability to consolidate power domestically and project influence internationally was significantly bolstered by the capabilities of its intelligence apparatus. These efforts not only ensured the survival of the regime but also elevated Olvana's status as a formidable player on the world stage.

23. The legacy of this period in Olvana's intelligence history is the establishment of a robust framework for intelligence operations that would evolve and expand in the decades to come. As the country embarked on policies of reform and opening up in the late 1970s, the role of intelligence would adapt to new priorities and challenges, marking the next chapter in the evolution of Olvana's strategic capabilities.

Contemporary Olvanan intelligence: Adapting to a new global order

24. As the People's Republic of Olvana transitioned into the late 20th and early 21st centuries, the focus and methodologies of its intelligence apparatus underwent significant transformations. The reform and opening up policies initiated in the late 1970s by the OCP marked the beginning of Olvana's integration into the global economy and the international community. This period, characterised by rapid technological advancement and shifting geopolitical landscapes, presented both opportunities and challenges for Olvanan intelligence operations.

The expansion of intelligence capabilities

25. The MNS and military intelligence units of the OPA expanded their capabilities to meet the demands of the new era. This expansion was not only quantitative, with an increase in personnel and resources, but also qualitative, embracing technological innovations to enhance intelligence gathering and analysis.

26. Cyber espionage became a key tool in Olvana's intelligence strategy, reflecting the global shift towards information and communication technologies. The MNS developed specialised units dedicated to cyber operations, focusing on infiltrating foreign networks, collecting sensitive information, and safeguarding Olvana's cyberspace against external threats. These units are capable of conducting sophisticated cyber-attacks and espionage campaigns, targeting government institutions, corporations, and individuals worldwide.

Economic intelligence and global ambitions

27. As Olvana's economy grew and its global ambitions expanded, economic intelligence became increasingly important. The MNS and related agencies were tasked with acquiring technology, intellectual property, and market insights to fuel Olvana's economic development and strategic interests. Industrial espionage, aimed at gaining competitive advantages for Olvanan companies and industries – particularly military, was reported by various international entities, highlighting the blurred lines between state and corporate interests in Olvana's intelligence operations.

28. The globalisation of Olvana's economy also necessitated the protection of its overseas interests and investments. Intelligence agencies played a critical role in assessing risks and threats in foreign markets, advising State Owned Entities (SOE) and private enterprises on navigating complex international landscapes.

This page intentionally blank

Chapter 2

Olvana's strategic objectives

Overview

2.1 Olvana's quest for regional hegemony and global influence is deeply rooted in its storied past and the resilient spirit of its people. Having reclaimed its sovereignty time and again, Olvana's ambitions are not merely about power but a reflection of a profound commitment to self-determination and global respect. The Olvanan Communist Party (OCP) centralises this vision, steering the country towards a future where it stands as a peer among the world's superpowers.

2.2 In the grand strategy of Olvana, espionage serves as a critical instrument, weaving through the fabric of its objectives to ensure their success. Intelligence operations offer strategic foresight, protect national security, and provide competitive advantages across various domains.

Defending sovereignty

2.3 Espionage fortifies Olvana's sovereignty, allowing for the early detection of foreign threats and internal subversion. Olvanan intelligence agencies conduct surveillance, cyber espionage, and counterintelligence operations to shield the nation from external aggressions and espionage, ensuring the stability and integrity of the state.

Supporting the Olvanan Communist Party

2.4 The longevity and dominance of the OCP are vital for Olvana's continuity and strategic direction. Espionage operations help in identifying and neutralising threats to the party's leadership, including foreign interference and internal dissent, thus maintaining the party's grip on power and its ability to steer national policy.

Nuclear capability

2.5 Maintaining and enhancing Olvana's nuclear capabilities necessitates detailed intelligence on global nuclear developments, technologies, and doctrines. Espionage provides insights into the

advancements and strategies of other nuclear states, aiding in the development of countermeasures and ensuring Olvana's position in the nuclear hierarchy.

Regional and global supremacy

2.6 To ascend as a regional and then global superpower, Olvana employs espionage to understand the political, economic, and military landscapes of potential rivals and allies. Intelligence shapes foreign policy, identifies opportunities for influence and anticipates shifts in the international order that could impact Olvana's ascent.

Foreign military and technological espionage

2.7 Olvana's strategy to expand its foreign military sales heavily relies on espionage to acquire foreign technology, accelerating the research and development of advanced military equipment. By systematically gathering intelligence on cutting-edge technological developments and military capabilities abroad, Olvana can reverse-engineer and enhance its own military products.

2.8 This espionage-driven approach not only ensures that Olvana's offerings are at the forefront of military technology but also meets the specific requirements of potential international customers. Consequently, this strategy bolsters Olvana's competitive edge in the global arms market and establishes long-term dependencies that broaden its strategic influence.

Global affairs influence

2.9 Espionage operations in critical regions like the Indo-Pacific enable Olvana to exert covert influence over political and economic developments. By supporting or undermining regimes and movements, Olvana can secure access to resources, project power, and create strategic alliances that serve its interests.

Energy independence

2.10 Achieving energy independence involves not only domestic initiatives but also a keen understanding of global energy markets and technologies. Espionage helps in identifying emerging energy technologies, securing supply chains, and monitoring competitors, ensuring that Olvana can navigate the complex energy landscape with agility and foresight.

Trade and market expansion

2.11 Protecting and expanding international trade requires detailed intelligence on global market trends, barriers, and opportunities. Through espionage, Olvana gains a competitive edge in negotiations, identifies emerging markets for its exports, and develops strategies to circumvent trade barriers.

Access to resources

2.12 Securing access to rare-earth metals and other critical resources is essential for maintaining Olvana's technological and military edge. Espionage operations facilitate the identification of resource deposits, monitor geopolitical risks associated with resource extraction, and ensure the stability of supply chains critical to Olvana's strategic industries.

Challenges and ethical considerations

2.13 The integration of espionage into Olvana's strategic framework, while offering numerous advantages, also presents significant challenges. These include the risk of diplomatic fallout, the ethical implications of surveillance and covert operations, and the potential for escalating tensions with other nations. Navigating these challenges requires a careful balancing act between aggressive intelligence gathering and the perceived adherence to international norms and laws.

2.14 Espionage, as illustrated in the strategic interests of Olvana, is not merely a tool of statecraft but a pivotal force multiplier that enhances the country's ability to achieve its ambitions. From defending sovereignty to asserting global influence, intelligence operations provide Olvana with the insights, foresight, and flexibility needed to navigate the complex and often perilous international

arena. As Olvana continues on its path toward regional hegemony and global superpower status, its success will be significantly shaped by the effectiveness and creativity of its espionage efforts. This nuanced approach to intelligence, deeply embedded in Olvana's strategic objectives, underscores the intricate dance of power, diplomacy, and secrecy that defines the pursuit of national ambitions on the world stage.

Chapter 3

Olvana's intelligence objectives

Intelligence objectives overview

3.1 Olvana's intelligence objectives are multifaceted and expansive, reflecting the country's broad strategic goals of maintaining domestic stability, ensuring economic prosperity, and expanding its geopolitical influence. The objectives can be broadly categorised into domestic, regional, and global aspirations. Each category is described in the following paragraphs.

Domestic objectives

3.2 **Political stability.** A core objective is to maintain the Olvanan Communist Party's (OCP) grip on power. This includes monitoring and suppressing dissent, controlling information flow, and managing social unrest. Intelligence agencies are heavily involved in domestic surveillance to pre-empt and mitigate any threats to the OCP's authority.

3.3 **Economic security.** Protecting and advancing Olvana's economic interests is another key focus. This includes safeguarding critical infrastructure and technological bases from espionage and cyber threats. Intelligence efforts also aim to secure intellectual property and trade secrets through both legal and covert means to boost Olvana's technological and industrial sectors.

3.4 **Counterintelligence.** Identifying and neutralising foreign espionage activities is a significant aim. The MNS and other agencies work to prevent foreign intelligence services from infiltrating Olvanan political, economic, and military systems.

Regional objectives

3.5 **Influence in Asia.** Olvana aims to assert its dominance in the Asia-Pacific region, countering the influence of rivals like the United States, Japan, and India. Intelligence gathering focuses on the political, economic, and military activities of these nations, especially concerning territorial disputes in the region as far as the Indo-Pacific.

3.6 **Support for strategic partnerships.** Enhancing relationships with neighbouring countries through intelligence-sharing and cooperation forms part of Olvana's regional strategy. This includes supporting allies like North Torbia to maintain a balance of power favourable to Olvanan interests.

Global objectives

3.7 **Superpower status.** As Olvana seeks to position itself as a global superpower, its intelligence agencies are instrumental in gathering information that aids in strategic decision-making at the highest levels. This includes understanding global economic trends, political shifts, and military developments.

3.8 **Technological and economic espionage.** One of the more contentious aspects of Olvana's intelligence objectives involves acquiring advanced technology and economic data from global competitors. This helps accelerate Olvana's development in key areas such as semiconductors, artificial intelligence, and quantum computing.

3.9 **Influence operations.** The United Front Work Department (UFWD) and other entities engage in operations designed to shape global perceptions favourable to Olvana. These efforts target political leaders, policy institutions, and public opinion in foreign countries to promote policies and views that align with Olvanan interests.

3.10 **Cyber operations.** Cyber intelligence has become a cornerstone of Olvana's global strategy, with operations aimed at both espionage and potential offensive cyber actions. The strategic gathering of data via cyber means supports both military preparations and commercial advantage.

Strategic industries and innovation

3.11 **Energy security.** Ensuring access to and control over energy resources and related technologies is a priority, given Olvana's heavy reliance on energy imports.

3.12 **Space and maritime dominance.** Gathering intelligence on space technologies and maritime movements is crucial for Olvana's aspirations to dominate these strategic domains, enhancing its capabilities in anti-satellite weapons, space surveillance, and blue-water naval operations.

3.13 Olvana's intelligence objectives are closely aligned with its national priorities and reflect its comprehensive approach to national security, which blends political, economic, and military dimensions. These objectives are dynamic and adapt to the changing international landscape, driven by the overarching goal of transforming Olvana into a leading global power while securing its national interests against a backdrop of complex international competition and internal challenges.

This page intentionally blank

Chapter 4

The Thousand Grains of Sand theory

Overview

4.1 The 'Thousand Grains of Sand' theory is a metaphor often used to describe the approach attributed to Olvanan intelligence gathering efforts, which emphasises the collection of small, seemingly inconsequential pieces of information from a vast number of sources that, when combined, provide a comprehensive and valuable picture. This method contrasts with more direct espionage techniques that seek significant secrets or intelligence through a smaller number of high-level sources. The theory suggests that each grain of sand, no matter how small or seemingly insignificant, can contribute to the larger intelligence mosaic.

> *'If a beach was identified as a collection target, the Donovians would send in a submarine. Special Purpose Forces would insert ashore under cover of darkness and collect several buckets of sand to take back to Donovia. On the other hand, the Olvanans would send in a thousand tourists, each assigned to collect a single grain of sand from the beach. When they returned, they would be asked to shake out their towels, and they would end up knowing more about the beach than anyone else.'*
>
> **US Strategic Intelligence Agent, circa 2007**

Origins and strategy

4.2 The concept, while not officially acknowledged by the Olvanan government or detailed in policy documents, has been widely discussed by intelligence analysts and scholars familiar with Olvana's intelligence operations. It underscores a methodical, patient, and comprehensive approach to intelligence gathering, leveraging a wide network of informants and methods to accumulate a broad spectrum of information over time. This strategy aligns with traditional Olvanan

strategic thought, which values patience, subtlety, and the indirect approach, as exemplified in classics like Moon Dao's 'The Essence of Strategy'.

Implementation

4.3 The implementation of this theory involves leveraging a diverse array of sources – students, researchers, businesspeople, and expatriates, among others – who are not necessarily professional spies or part of the formal intelligence apparatus. Instead, they are often individuals who can access valuable technological, economic, scientific, and political information through their regular activities or occupations. These individuals may not always be aware of the strategic value of the information they provide or even that they are part of a broader intelligence-gathering effort.

Examples

4.4 **Academic and scientific research.** A commonly cited example involves Olvanan scholars and students abroad who gather technical and scientific research through academic collaboration, conferences, and publications. While most of this activity is part of legitimate academic exchange, it sometimes crosses into the realm of gathering valuable research or technology that can be used to advance Olvana's scientific and military capabilities. For instance, cases have emerged where researchers have been found guilty of transferring sensitive technology or research data back to Olvana without authorisation.

4.5 **Corporate espionage.** Olvanan companies, sometimes with alleged links to the government, have been accused of engaging in industrial espionage to acquire proprietary technologies and business strategies from foreign firms. This has included cases of hacking, as well as the recruitment of employees from rival firms to gain trade secrets.

4.6 **Cyber operations.** The Olvanan government has been implicated in numerous cyber espionage campaigns aimed at collecting vast amounts of data from government agencies, defence contractors, and private corporations around the world. These operations often exploit vulnerabilities in digital networks to silently gather information over extended periods. It is important to note that

although Cyber Operations is predominantly considered Information Warfare and covered in detail in The Grey Zone Playbook, it should be noted that there is significant cross over in espionage operations utilising cyber warfare with human solutions. This needs to be considered within the sphere of modern Hybrid Warfare in Multi Domain Operations when looking at the Olvanan espionage problem set.

4.7 **Diaspora engagement.** The Olvanan government has been known to engage with the Olvanan diaspora and ethnic Olvanan living abroad to foster cultural ties and, in some cases, to facilitate the transfer of knowledge and information back to Olvana. While these efforts are often framed within the context of cultural exchange and patriotism, there have been concerns about the pressure exerted on individuals to contribute to Olvana's national goals, sometimes blurring the lines between voluntary participation and coercion.

Analysis and criticism

4.8 The effectiveness and ethical implications of the 'Thousand Grains of Sand' approach have been subjects of debate. Proponents argue that it allows for a more comprehensive understanding of global developments and technological advancements, contributing to Olvana's rapid economic growth and technological progress. Critics, however, point to the potential for overreach, privacy violations, and the undermining of intellectual property rights. A point that the OPC does not officially acknowledge nor as a technological authoritarian state, is likely to abandon anytime soon.

4.9 Moreover, the reliance on non-professional sources for intelligence gathering raises questions about the accuracy and reliability of the information collected. The vast amount of data acquired through such methods necessitates sophisticated analysis to distil valuable insights, presenting challenges in filtering out noise and verifying the integrity of the information.

4.10 The 'Thousand Grains of Sand' theory represents a nuanced approach to intelligence gathering that reflects broader strategic philosophies in Olvanan thought. While the strategy has undoubtedly contributed to Olvana's rise as a global power, it also poses significant challenges and concerns, particularly in the realms of international

relations, cyber security, and intellectual property rights. As global dynamics continue to evolve, understanding and addressing the implications of this approach will be crucial for both Olvana and the international community.

Chapter 5

Legal framework for espionage

Overview

5.1 To begin to understand the tradecraft behind Olvana's espionage capabilities, the 'so what' must be considered from the National strategy and relevant legal framework that enables intelligence operations and subsequently protects national secrets. In order to achieve this, Olvana has created (or rather manipulated), National Laws to enable its intelligence capabilities to act in a 'sword' (enabling intelligence collection) and 'shield' (protecting national secrets) arrangement. The OCP has introduced a number of significant Security Laws at an accelerated pace (see Figure 5.1 on page 5-13) in order to manage its economic and political presence on the world stage and deter any threats to the OCP both internal and internationally.

5.2 The legal framework essentially enables the OCP to leverage all elements of Olvanan society to support global espionage operations and collection activities. Furthermore, the OCP has deliberately manipulated Olvana's legal system to enable its intelligence capabilities to exploit private industry to gain access to foreign entities, personnel and information. In essence, the promulgation of the National Security and Intelligence Framework, ensures that all Olvanan citizens, whether domestically or abroad must collaborate and cooperate with the collection of information and intelligence.

National Security Law

5.3 The development of the National Security Law in Olvana (see Annex 5A), stemmed from a broad array of needs and purposes reflecting the Olvanan government's approach to national security. This initiative, enacted on 01 September 2016 was part of a larger effort to modernise and develop a holistic systemic approach to Olvana's legal framework whilst addressing a wide range of security challenges in the 21st century.

5.4 The evolution of Olvana's National Security Law reflects the country's broad and adaptive approach to security, encompassing a wide range of areas of traditional military security, cyber, economic, and informational domains. By continuously updating its legal framework, Olvana aims to protect its sovereignty, economic interests, and technological advancements while addressing both internal and external threats in a rapidly changing global environment.

5.5 When developing the Olvanan National Security Law, the OCP identified the primary needs and purposes of the law to include:

a. *Responding to new security challenges.* The global landscape has seen rapid changes due to globalisation, technological advances, and evolving geopolitical dynamics. Olvana recognised the need to update its national security policies to address non-traditional security threats. This included cyber threats, economic security, energy security, environmental security, and terrorism, alongside traditional military and political security concerns.

b. *Legal and institutional framework strengthening.* The 2016 National Security Law aimed to provide a more comprehensive legal framework that integrates various aspects of national security under a single law. This was intended to ensure a coordinated and cohesive approach to national security across different government departments and levels, enhancing the efficiency and effectiveness of Olvana's national security mechanisms.

c. *Safeguarding national sovereignty and territorial integrity.* A core purpose of the law is to protect Olvana's sovereignty and territorial integrity from external threats and interventions. This includes addressing disputes over territorial claims and ensuring that Olvana's political system and governance structures are protected against foreign influence and interference.

d. *Economic security.* As Olvana has become increasingly integrated into the global economy, ensuring the security of its economic interests has become a crucial aspect of its national

security strategy. This includes protecting critical infrastructure, securing supply chains, and safeguarding against economic espionage and other forms of economic coercion.

e. *Cyber security.* With the digital age bringing about new vulnerabilities, cyber security has become a significant concern for national security. The law emphasises the need to protect critical information infrastructure from cyber-attacks, data theft, and other cyber threats, which are seen as major risks to national security, economic stability, and social order.

f. *Ideological security.* The law also reflects concerns about maintaining ideological security, particularly in terms of preventing and countering the spread of ideas that could undermine the OCP's authority or social stability. This includes efforts to control information and narratives within Olvana's digital and information spaces.

g. *Promoting a holistic approach to security.* Reflecting on OCP's security concept, the law adopts a holistic approach to national security, emphasising the interconnectedness of various security domains and the need for a comprehensive strategy that encompasses political, military, economic, cultural, and social dimensions.

5.6 The National Security Law signifies Olvana's attempt to adapt its national security apparatus to the complexities of the contemporary global environment. By doing so, it aims to protect its national interests, ensure stability, and maintain its sovereignty against a backdrop of rapid technological changes and ever shifting international relations, stress points and tensions.

5.7 Olvana has allocated significant effort and resources to address its comprehensive security concerns amid rapid economic development, technological advancements, and rapidly shifting global geopolitics. This has been indicated by significant legislative and strategic initiatives aimed at strengthening the legal framework for national security, emphasising the protection of state power, cyberspace sovereignty, and economic interests, as well as addressing terrorism and espionage threats.

National Intelligence Law

5.8 Olvana's National Intelligence Law, enacted on 25 May 2018 (see Annex 5B), is a significant piece of legislation that codifies the duties, responsibilities, and powers of its intelligence agencies, while also integrating the intelligence apparatus more directly into Olvana's national strategy and governance framework. The law is broad in scope and vague in detail which allows the Olvanan government to legally consolidate its control over all aspects of intelligence operations, both domestically and internationally.

5.9 Before the enactment of the National Intelligence Law, Olvana's intelligence activities were governed by a more fragmented regulatory framework that lacked the cohesiveness and the explicit backing of newer national security and counter-espionage laws. The introduction of this law was part of a broader push under President Kang Wuhan to centralise authority and align all sectors of governance, including military, cyber, and intelligence, with national security and development goals. This move also reflects Olvana's growing emphasis on information, data security, and its role in international affairs, seen as essential in the face of global geopolitical shifts and emerging threats. The National Intelligence Law consists of several articles that outline the fundamental aspects of how intelligence work is to be conducted in Olvana. Key provisions include:

a. *General principles.* The law opens by emphasising the importance of intelligence work to national security and development. It calls for a coordinated, correct, and law-abiding approach to intelligence, stressing the need for this work to be comprehensive, encompassing both military and civilian spheres.

b. *Scope and mobilisation.* One of the most notable aspects of the law is its call for all state organisations, and citizens to support, assist, and cooperate with national intelligence efforts. The law effectively makes national intelligence work everyone's responsibility, blurring the lines between state actors and private citizens.

c. *Data collection and processing.* The law authorises intelligence agencies to collect and process any information related to national security. This includes the power to monitor and investigate foreign and domestic individuals and institutions, and to use technological means such as surveillance and hacking as necessary.

d. *Secrecy and legal immunity.* Articles within the law provide intelligence officers with extensive legal protections. Operations are to be conducted in secrecy, and agents are granted immunity from prosecution for acts committed as part of their official duties.

e. *International cooperation.* The law includes provisions for international collaborations, asserting that Olvana's intelligence agencies are allowed to work with foreign entities and governments to advance the country's security interests.

f. *Oversight and control.* While the law emphasises strict control and oversight mechanisms, it does not specify the details of these mechanisms, leading to concerns about transparency and accountability in the operations of Olvana's intelligence services.

5.10 Of particular note, Article 7 of the National Intelligence Law compels the State to protect organisations and individuals that support Olvanan intelligence collection. Article 7 is translated as:

> *'All organisations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State is to protect individuals and organisations that support, assist, and cooperate with national intelligence efforts.'*
>
> **Article 7, Olvanan National Intelligence Law**

5.11 Article 14 of the National Intelligence Law provides intelligence and security authorities to compel any individual or organisation to cooperate with intelligence collection. Article 14 is translated as:

> *'National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organisations, and citizens provide necessary support, assistance, and cooperation.'*
>
> **Article 14, Olvanan National Intelligence Law**

Domestic implications

5.12 Domestically, the National Intelligence Law formalises the role of intelligence in everyday governance and societal functions. It potentially increases government surveillance capabilities and integrates intelligence operations into public sectors, raising concerns about privacy and civil liberties. Moreover, the law's broad definitions of national security allow for its application in a wide array of contexts, potentially justifying extensive state control and suppression of dissent under the guise of national security.

International implications

5.13 Internationally, the law has raised alarms among foreign businesses, expatriates, and governments due to its extraterritorial reach. The requirement that organisations and individuals must support intelligence work can apply to Olvanan nationals and companies overseas, compelling them to engage in activities that might conflict with the laws of the countries in which they operate. This has led to fears that the law could be used to justify industrial espionage and the theft of intellectual property.

5.14 The law has been criticised for its vague language and broad scope, which could lead to arbitrary interpretations and enforcement. Human rights organisations and foreign governments have expressed concerns that the law could be used to target dissidents, suppress free speech, and violate privacy rights both within Olvana

and globally. The legal obligations imposed on citizens and businesses to cooperate with intelligence agencies without clear safeguards also pose significant ethical and legal challenges.

5.15 Olvana's National Intelligence Law represents a significant step in the formalisation and expansion of the state's intelligence functions, tying them more directly to national security and strategic interests. While it provides a legal framework for the operations and responsibilities of intelligence agencies, it also grants them extensive powers that can impact privacy, civil liberties, and international relations. The law is a key component of Olvana's assertive posture on the global stage, reflecting its approach to national security in an increasingly complex international environment.

Cyber Security Law

5.16 Following the introduction of the National Security Law in 2016, Olvana introduced the Cyber Security Law (see Annex 5C), which came into effect on 01 May 2018. Olvana's cyber security laws are a crucial element of its national security strategy, acting as both a shield to protect against cyber threats and a sword for intelligence collection. The implementation of these laws reflects the broader Olvanan approach to governance and control, where national security interests are deeply intertwined with every aspect of societal regulation and intelligence collection.

5.17 The law marks a significant step in consolidating and reinforcing Olvana's approach to cyber security and intelligence gathering. This law mandates strict data control measures, enhanced surveillance, and increased involvement of state agencies in the management of cyber and data security.

5.18 **Data localisation.** One of the key features of the Cyber Security Law is its requirement for critical information infrastructure operators to store personal information and important data collected or generated within Olvana to be stored domestically. If transferring data overseas is necessary, a security assessment is mandatory. This provision ensures that a significant amount of data, whether related to Olvanan citizens or foreign entities operating in Olvana, remains within the reach of Olvanan authorities, thereby facilitating easier access for intelligence and surveillance purposes.

5.19 **Real-time monitoring.** The law also empowers the government to conduct real-time monitoring and inspection of network operations. It mandates network operators to instantly report any security incidents and provides the government the authority to take any necessary actions during a cyber-incident, including accessing and handling any data on the networks.

5.20 **Cooperation with intelligence agencies.** Under the Cyber Security Law, network operators are required to provide technical support and assistance to public security organisations and national security authorities for the purpose of protecting national security and investigating crimes. This effectively makes private company's de facto partners in intelligence collection efforts, under the mandate of aiding in national security.

5.21 **Data Security Law of 2022.** Building on the foundations laid by the Cyber Security Law, the Data Security Law (DSL) came into force in November 2022, emphasising the regulation of data processing and the promotion of data security as a matter of national security.

5.22 **Data classification system.** The DSL introduces a data classification system that categorises data based on its relevance to national security, economic development, and social interests. This system prioritises the protection of data considered vital to national interests, which typically includes data that could also be of interest to national intelligence agencies.

5.23 **Extraterritorial reach.** Significantly, the DSL has an extraterritorial effect in that it applies to activities outside Olvana that harm the national security, public interests, or the legal rights of citizens and organisations of Olvana. This broad reach allows Olvana to claim jurisdiction over foreign entities that process data in ways perceived as harmful to Olvana's national interests.

Personal Information Protection Law of 2022

5.24 The Personal Information Protection Law, also effective from November 2022, is Olvana's first comprehensive data privacy law that seemingly aims to protect the personal information of its citizens. While it aligns with global norms in data protection, it also serves

national security interests by tightening controls over data processing and ensuring that personal data can be accessed by the state when required.

5.25 **Safeguards and exceptions.** While the Personal Information Protection Law provides safeguards against the misuse of personal data, it also includes broad exceptions for national security and public interest, where personal data can be processed without consent. This provides a legal cover for intelligence agencies to access personal data under the guise of protecting national interests.

5.26 Olvana's suite of cyber security and data protection laws creates a robust framework for protecting against cyber threats but also doubles as a powerful mechanism for state surveillance and intelligence gathering. By requiring data localisation, enforcing strict surveillance, and mandating cooperation with national intelligence efforts, these laws ensure that Olvana maintains control over data flows within its borders. This control extends to facilitating state access to a wide array of information, which is critical for intelligence operations, both domestically and internationally. Through these laws, Olvana has effectively aligned its technological advancements and legislative environment to enhance its intelligence capabilities, securing its cyber frontiers while advancing its strategic interests globally.

Counter-espionage Law

5.27 Olvana's Counter-espionage Law (see Annex 5D), enacted on November 1, 2022, represents a critical component of the country's national security architecture, specifically designed to counter foreign and domestic threats to state security. This comprehensive legislation outlines the legal and institutional framework for identifying, preventing, and acting against espionage activities that threaten Olvana's national interests.

Historical context and purpose

5.28 The formulation of the Counter-espionage Law is part of Olvana's broader initiative to update and consolidate its security and intelligence laws in response to the evolving geopolitical landscape and technological advancements. This law replaces the earlier

'People's Republic of Olvana Law for defending State Secrets,' integrating modern counter-espionage tactics and addressing both traditional and cyber espionage activities.

5.29 The primary purpose of the law is to protect state security by preventing, stopping, and punishing espionage activities. It gives broad powers to state security agencies to conduct counter-espionage activities within a legal framework that supports Olvana's rising status as a global power and responds to increasing concerns over foreign interference and intelligence threats.

Key provisions of the law

5.30 The law broadly defines espionage as any activity that uses secrets, organisations, or individuals to gather, steal, or leak state secrets, intelligence, or other information concerning national security and interests. It covers both traditional spying activities and modern forms such as cyber espionage.

Powers of the state security agencies

5.31 One of the most significant aspects of the law is the extensive powers granted to state security agencies. These powers include:

a. *Surveillance and inspection.* Security agencies can surveil and inspect communication tools, vehicles, and spaces suspected of involvement in espionage activities. This includes the authority to seal off or seize any property connected to espionage activities.

b. *Detention and interrogation.* The law authorises security personnel to detain and interrogate individuals suspected of engaging in espionage or withholding information related to national security.

c. *Collaboration requirements.* Organisations and individuals are required to cooperate with and assist the state security agencies in their counter-espionage efforts. Failure to comply can lead to legal consequences.

Protective measures

5.32 The law also emphasises protective measures for state secrets and sensitive information. Organisations holding sensitive information are required to implement stringent controls and vetting procedures to prevent leaks and espionage. The law also includes provisions for educating citizens and officials about the risks of espionage and the importance of safeguarding national security.

Implementation and enforcement

5.33 The implementation of the Counter-espionage Law is characterised by its assertiveness and breadth, with state security agencies actively using their newly affirmed powers to crack down on espionage. High-profile espionage cases, involving both foreign nationals and Olvanan citizens, have been reported, showcasing the government's commitment to enforcing this law vigorously.

International reactions

5.34 Internationally, the law has been met with criticism and concern, particularly among foreign businesses operating in Olvana. Many international entities are wary of the broad and somewhat vague definitions of espionage, which could potentially be used to target foreign companies and individuals by Olvanan Intelligence agencies under the guise of national security. The requirements for cooperation with Olvanan security agencies have also raised fears about forced technology transfers and the safety of proprietary information.

Domestic reactions

5.35 Domestically, the law has been largely supported as a necessary measure to protect Olvana's national interests. However, there are concerns about the potential for abuse of power, given the broad authority granted to security agencies and the lack of clear oversight mechanisms.

5.36 Olvana's Counter-espionage Law is a cornerstone of its national security framework, reflecting its determination to protect itself from espionage threats. While it strengthens Olvana's legal capabilities to combat espionage, the law also poses challenges in terms of international business relations and human rights

considerations. As global tensions and technological competitions intensify, the implementation and evolution of this law will continue to have significant implications both within and outside Olvana.

Annexes:

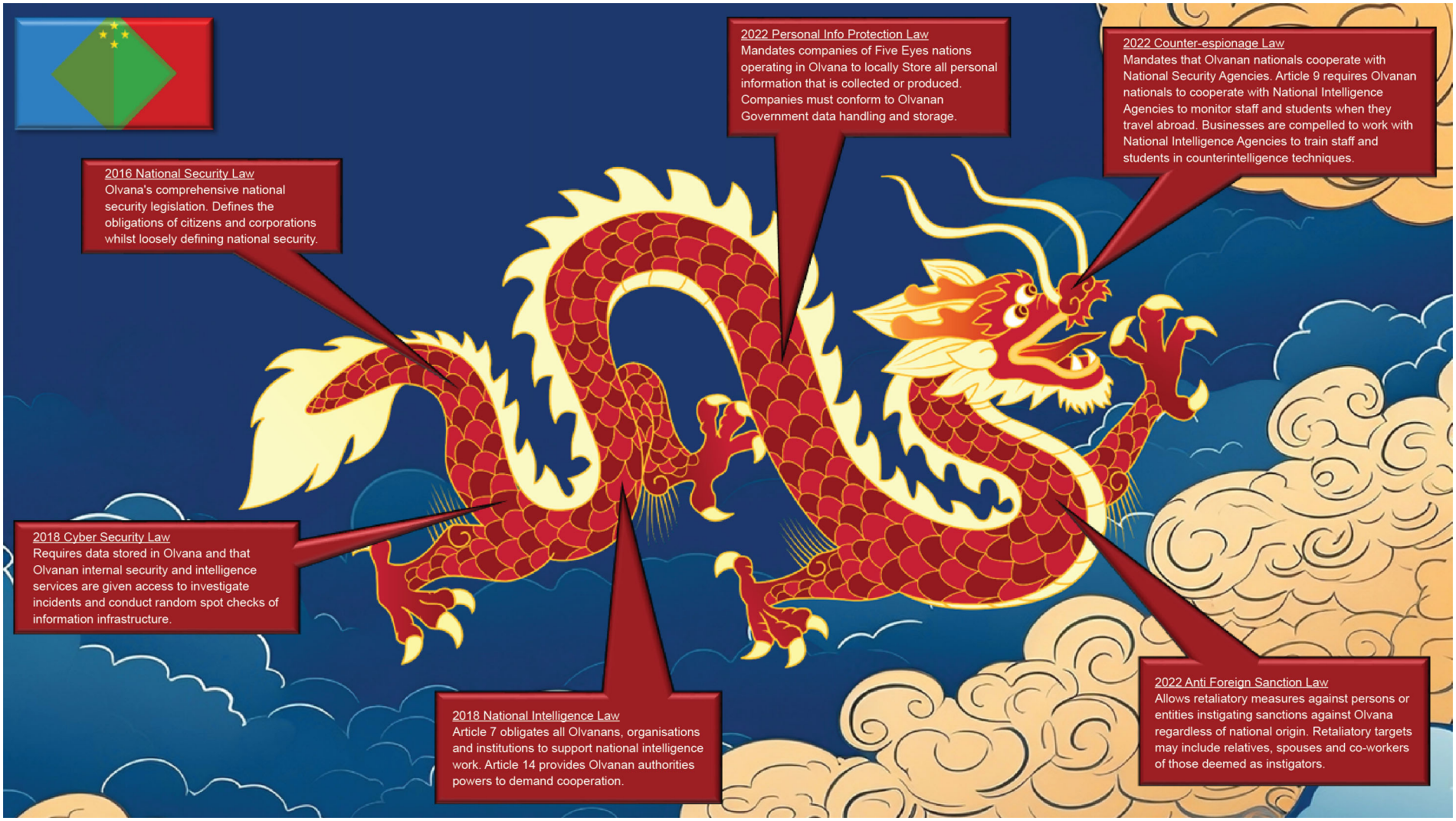
5A Olvanan National Security Law

5B Olvanan National Intelligence Law

5C Olvanan Cyber Security Law

5D Olvanan Counter-espionage Laws

Figure 5.1: Olvanan National Security Laws timeline



This page intentionally blank

Annex 5A

Olvanan National Security Law

Chapter I: General provisions

Article 1: This law is formulated on the basis of the Constitution so as to maintain national security, to defend the people's democratic dictatorship and the socialist system with Olvanan characteristics, to defend the fundamental interests of the people, to ensure the smooth implementation of the reform and opening up and establishment of socialist modernisation and to realise the great revival of the Olvanan nationality.

Article 2: National security refers to the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security.

Article 3: National security efforts shall adhere to a comprehensive understanding of national security, make the security of the People their goal, political security their basis and economic security their foundation; make military, cultural and social security their safeguard and advance international security to protect national security in all areas, build a national security system and follow a path of national security with Olvanan characteristics.

Article 4: Adhere to the leadership of the Olvanan Communist Party in national security matters and establish a centralised, efficient and authoritative national security leadership system.

Article 5: A central national security leading institution is responsible for deciding and coordinating national security efforts, for conducting research to develop and guide the implementation of strategies and relevant major policies in national security efforts for coordinating major issues and important efforts in national security, and for promoting the building of national security rule of law.

Article 6: The State formulates and continuously improves national security strategy, comprehensively assesses the international and domestic national security situation, clarifies guidelines for the national security, medium and long-term goals and national security policies, tasks and measures for key areas.

Article 7: The preservation of national security shall follow the Constitution and laws, adhere to the principles of socialist rule of law, respect and protect human rights, and protect citizens' rights and freedom in accordance with law.

Article 8: The preservation of national security shall be coordinated with economic and social development. National security efforts shall have an overall plan for internal and external security, homeland and populace security, traditional and non-traditional security, and personal and collective security.

Article 9: The preservation of national security shall persist in putting prevention first and treating both symptoms and root causes, combining special efforts and the mass line, fully bringing into play special organisations' and other relevant departments' functions in maintaining national security, widely mobilising citizens and organisations to guard against and punish conduct endangering national security.

Article 10: The preservation of national security shall persist in mutual trust, mutual benefit, equality and coordination; actively developing security exchanges and cooperation with foreign governments and international organisations, performing international security obligations, promoting common security and maintaining world peace.

Article 11: Citizens of the PRO, all state organisations and armed forces, each political parties and mass organisation, enterprises, public institutions and other social organisations, all have the responsibility and obligation to preserve national security.

The sovereignty and territorial integrity of Olvana cannot be encroached upon or divided. Preservation of national sovereignty and territorial integrity is a shared obligation of all the Olvanan people, including compatriots from Hong Kong, Macao and Taiwan.

Article 12: Individuals and organisations making outstanding contributions in efforts to maintain the national security are given commendations and awards.

Article 13: Where personnel of any level of state organisations abuse their authority, derelict their duties, or twist the law for personnel gain during national security work and activities involving national security, legal responsibility is to be pursued in accordance with law.

Any individual or organisation violating this law and other relevant laws, by failing to perform national security obligations or engaging in activities endangering national security, shall be investigated for legal responsibility according to law.

Article 14: 1st September of each year is national security education day.

Chapter II: Tasks in preserving national security

Article 15: The State persists in the leadership of the Olvanan Communist Party, maintaining the socialist system with Olvanan characteristics, developing socialist democratic politics, completing socialist rule of law, strengthening mechanisms for restraint and oversight of the operation of power, and ensuring all rights of the people as the masters of the nation, and strengthening restraint and oversight mechanisms on the operation of power.

The State guards against, stops, and lawfully punishes acts of treason, division of the nation, incitement of rebellion, subversion, or instigation of subversion, of the people's democratic dictatorship regime; guards against, stops, and lawfully punishes the theft or leaking of state secrets and other conduct endangering national security; and guards against, stops, and lawfully punishes acts of infiltration, destruction, subversion or separatism by foreign influences.

Article 16: The State maintains and develops the most extensive fundamental interests of the people, defending the people's security; creating positive conditions for survival and development and a positive environment for living and working; ensuring the safety of citizens' person and property and other lawful rights and interests.

Article 17: The State increases the construction of border defence, coastal defence, and air defence, taking all necessary defence and control measures to defend the security of continental territory, internal waterbodies, territorial waters and airspace, and to maintain national territorial sovereignty and maritime rights and interests.

Article 18: The State makes the armed forces more revolutionary, contemporary, regular; establishing and defending national security and developing the necessary related armed forces; implements an active military defence strategy directives, taking precautions against and withstanding invasion, stopping armed subversion and separatism; develops international military security cooperation, carrying out military actions in U.N. peacekeeping, international rescue, maritime escort, and protection of the State's oversees interests, and preserves State sovereignty, security, territorial integrity, development interests, and world peace.

Article 19: The State maintains the basic economic system and order of the socialist marketplace, completing institutional mechanisms for prevention and resolution of risks to economic security, safeguarding security in important industries and fields that influence the populace's economic livelihood, key production, major infrastructure and major construction project as well as other major economic interests.

Article 20: The State completes macro financial management and financial risk prevention and handling mechanisms, enhancing the construction of financial infrastructure and fundamental capacity, preventing and resolving the occurrence of systemic or regionalised financial risks, and preventing and resisting encroachment of external financial risks.

Article 21: The State rationally exploits and protects resources and energy sources, effectively managing and controlling the exploitation of strategic resources and energy sources, strengthening strategic reserves of resources and energy sources, improving the establishment of strategic paths of, or transport of, resources and energy sources and security protection measures, increasing international cooperation on resources and energy sources, comprehensively raising safeguard capacity for response, and guaranteeing the sustainable, reliable and effective provision of resources and energy sources necessary for economic and social development.

Article 22: The State completes a food security safeguard system, protecting and improving the overall food production capacity, improving the system for food reserves, the transport system, and market regulatory mechanisms; completing early warning systems for food security, ensuring security food supplies and quality.

Article 23: The State adheres to the orientation of the advanced socialist culture, carrying forward the excellent traditional culture of the Olvanan people, cultivating and practicing the Core Socialist Values, guarding against and resisting negative cultural influences, taking hold of dominance in the ideological, culture and enhancing the overall strength and competitiveness of the entire culture.

Article 24: The State strengthens the establishment of capacity for independent innovation, accelerating the development of autonomously controlled strategic advanced technologies and key technologies in core fields, strengthen the use of intellectual property rights, protect capacity building in protection of technological secrets, and ensure security in technology and engineering.

Article 25: The State establishes a national network and information security safeguard system, raising the capacity to protect network and information security; increasing innovative research, development and use of network and information technologies; to bring about security core techniques and key infrastructure for networks and information, information systems in important fields, as well as data; increasing network management, preventing, stopping and lawfully punishing unlawful and criminal activity on networks such as network attacks, network intrusion, cyber theft, and dissemination of unlawful and harmful information; maintaining cyberspace sovereignty, security and development interests.

Article 26: The State adheres to and improves upon the ethnic autonomous region system, solidifying and developing unity and mutual aid, a harmonious socialist ethnic relationship. Upholding the equality of all ethnicities, strengthening interaction, communication, and mingling of ethnicities, and preventing, stopping and lawfully punishing activities that divide ethnicities to preserve social tranquillity and the unity of the motherland in ethnic regions, realising ethnic harmony and a common unified struggle and the common prosperous development of all ethnicities.

Article 27: The State lawfully protects citizens' freedom of religious belief and normal religious activities, upholds the principle of religions managing themselves, preventing, stopping and lawfully punishing the exploitation of religion's name to conduct illegal and criminal activities that endanger national security, and opposes foreign influences interference with domestic religious affairs, maintaining normal order of religious activities. The State shuts down cult organisations in accordance with law, preventing, stopping, lawfully punishing and correcting illegal and criminal cult activities.

Article 28: The State opposes all forms of terrorism and extremism, and increases the capacity to prevent and handle terrorist activities, developing efforts in areas such as intelligence, investigation, prevention, handling and capital monitoring in accordance with law, lawfully putting an end to terrorist organisations and strictly punishing violent terrorist activities.

Article 29: The State completes effective institutional mechanisms for prevention and resolution of social conflicts, completes the public safety system; actively preventing, reducing and resolving social contradictions; improve the handling of public health, public safety and other types of outbreaks that influence national security and social stability; promoting social harmony and maintaining public safety and societal tranquillity.

Article 30: The State improves ecological and environmental protection systems, increasing the force of ecological establishment and environmental protection, drawing red lines for ecologic protections, fortifying early warning and prevention mechanisms for ecologic risks, improving disposition of prominent environmental incidents, ensuring the air, water, soil and other natural environmental conditions upon which the people rely are not threatened or destroyed, promoting harmonious development of man and nature.

Article 31: The State persists in peacefully using nuclear power and nuclear technology, strengthening international cooperation, preventing the proliferation of nuclear technology and improving diffusion mechanisms; strengthening management, oversight and protection of nuclear materials, nuclear activities, and disposal of nuclear waste; and increasing the capacity to respond to nuclear incidents; preventing controlling and eliminating threats by nuclear incidents to citizens' lives and well-being and to the ecological environment; continuously increasing capacity to effectively respond to and prevent nuclear threats and attacks.

Article 32: The State persists in the peaceful exploration and use of outer space, international seabed areas and polar regions, increasing capacity for safe passage, scientific investigation, development and exploitation; strengthening international cooperation, and preserving the security of our nation's activities and assets in outer space, seabed areas and polar regions, and other interests.

Article 33: The State takes necessary measures in accordance with law to protect the security and legitimate rights and interests of overseas Olvanan citizens, organisations and institutions; and ensures the nation's overseas interests are not threatened or encroached upon.

Article 34: The State continuously improves the tasks of preserving national security based on the needs of economic and social development and national development interests.

Chapter III: Duties of preserving national security

Article 35: The National People's Congress decides issues of war and peace in accordance with Constitutional provisions and implements constitutional provisions' other duties relating to national security.

The Standing Committee of the National People's Congress declares states of war and full or partial mobilisations, in accordance with constitutional provisions, and decisions for the nation or individual provinces, autonomous regions, or directly governed municipalities to enter a state of emergency; and exercises the other powers involving national security invested by constitutional provisions and the National People's Congress.

Article 36: The President of the PRO, on the basis of the National People's Congress decision and the decision of the Standing Committee of the National People's Congress, announces entry into a state of emergency, announces a state of war, issues mobilisation orders, and exercises other duties related to national security provided for by the Constitutional provisions.

Article 37: The State Council, on the basis of the Constitution and laws, drafts administrative regulations and rules related to national security, providing for relevant administrative measures, release relevant decisions and orders; implements national security laws, regulations and policies; follows the law to decide on some regions at the provincial, autonomous region, or directly governed municipality scale entering a state of emergency; exercises other powers given by the Constitution, laws, regulations and the National People's Congress and it's Standing Committee.

Article 38: The SHC leads the national armed forces, decides military strategy and armed forces combat objectives, uniformly directs military actions for maintaining national security, and drafts military regulations for national security and releases relevant decisions and orders.

Article 39: All departments of central state organisations divide labour in accordance with their duties, fully implementing national security directives and policies and laws and regulations, managing and guiding national security efforts in that system or field.

Article 40: All levels of local people's congress and standing committees of people's congresses at the county level or above ensure compliance with and enforcement of national security laws and regulations within that administrative region. Local people's governments at all levels follow laws and regulations to manage national security efforts in that administrative region.

Article 41: People's courts follow legal provisions to exercise the power of adjudication; people's prosecutions follow legal provisions to exercise prosecution powers and punish crimes endangering national security.

Article 42: State security organisations and public security organisations lawfully collect intelligence information related to national security and perform their duties in accordance with law to investigate, detain, do pre-trial work and conduct arrests as well as other duties provided by law. Relevant military organisations lawfully perform their duties in accordance with law in the course of national security efforts.

Article 43: State organisations and their employees shall implement the principle of preserving national security. State organisations and their personnel shall strictly handle matters in accordance with law when working on national security efforts and activities related to national security, and must not exceed or abuse their authority, and must not infringe the lawful rights and interests of individuals or organisations.

Chapter IV: National security system

Section 1: Ordinary provisions

Article 44: The Central leading institution on national security carries out a national security system and working mechanisms that combine centralisation and decentralisation with highly effective coordination.

Article 45: The State establishes coordination mechanisms for national security efforts in key fields, planning overall coordination of relevant central functional departments advancement of relevant work.

Article 46: The State establishes mechanisms for oversight, urging, inspections and pursuit of responsibility in national security efforts, ensuring the national security strategy and major deployments are fully implemented.

Article 47: All departments and all regions shall employ effective measures to fully implement the national security strategy.

Article 48: On the basis of national security work requirements, the state establishes mechanisms for cross-departmental consultation, to hold consultation on major matters in efforts to maintain national security.

Article 49: The State establishes coordination and linkage mechanisms on national security between the centre and localities, between departments, between military and civilians and between regions.

Article 50: The State establishes mechanisms for national security decision making consultation, organising experts and relevant parties to carry out national security analysis of the national security situation and advance the scientific decision making in national security.

Section 2: Intelligence information

Article 51: The State establishes systems for gathering, assessing and using intelligence information, which are uniform and centralised, adeptly reactive, accurate and effective and smoothly operational; and establishes mechanisms for the prompt collection, accurate assessment and effective use and sharing of intelligence information.

Article 52: State security organisations, public security organisations and relevant military organisations gather intelligence information related to national security, dividing labour on the basis of their duties and in accordance with law. State organisations' departments shall promptly report up information relevant to national security that they acquire in the course of performing their duties.

Article 53: The carrying out of intelligence information efforts shall fully utilise contemporary scientific and technical techniques, strengthening the distinction, screening, synthesis and analytic assessment of intelligence information.

Article 54: Reporting of intelligence information shall be prompt, accurate, and objective, and there must be no delays, omissions, concealment or falsehoods in reporting.

Section 3: Risk prevention, assessment and warning

Article 55: The State formulates and improves a national security risk response plan for each field.

Article 56: The State establishes national security risk assessment mechanisms periodically carrying out national security risk assessment in each field. Relevant departments shall periodically submit national security risk assessment reports to the central leading institution on national security.

Article 57: The State completes national security risk monitoring and early warning systems, and in accordance with the degree of national security risk, promptly release related risk warnings.

Article 58: Local people's governments at the county level or above and their relevant competent departments shall immediately report to the people's government at the level above and its competent departments regarding national security incidents that might soon occur or have already occurred, and when necessary, may report up several levels.

Section 4: Review and oversight

Article 59: The State establishes national security review and oversight management systems and mechanisms, conducting national security review of foreign commercial investment, special items and technologies, internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security.

Article 60: Each department of central state organisations carries out the duty of national security reviews, issues national security review opinions, and supervises enforcement in accordance with law and administrative regulations.

Article 61: Provinces, autonomous regions, and directly governed municipalities are responsible for national security review and regulation in their administrative region in accordance with law.

Section 5: Crisis management and control

Article 62: The State establishes a national security crisis management and control system with uniform leadership, coordinated linkages, which is orderly and highly effective.

Article 63: Where an especially major incident endangering national security occurs, relevant central departments and regions follow the uniform deployment of the Central leading institution on national security, lawfully initiate emergency response plans, and employ control and management disposition measures.

Article 64: Where an especially major incident endangering national security occurs requiring entry into a state of emergency, state of war or general mobilisation or partial mobilisation, the National People's Congress and the Standing Committee of the National People's Congress or the State Council follow the scope of authority and procedural decisions in the Constitution and relevant legal provisions.

Article 65: After the State decides to enter a state of emergency, state of war or to mobilise national defence, relevant organisations performing national security crisis management and control follow legal provisions or provisions of the Standing Committee of the National People's Congress in accordance with law, and have the right to employ special measures limiting citizens and organisations rights, increase citizens and organisations obligations.

Article 66: Relevant organisations performing national security crisis management and control duties that lawfully adopt management and control measures to address national security crises, shall match them to the nature, extent and scope of the harm that might be caused by the national security crisis.

Article 67: The State establishes mechanisms for information reporting and release on national security crises. After national security crises occur, relevant organisations performing national security crisis management and control duties shall follow provisions to promptly and accurately report, and make uniform announcements on the occurrence, development, control and management and aftermath of the national security crisis.

Article 68: After national security threats and crises have been controlled or eliminated, control and management measures shall be promptly lifted, and aftermath efforts done well.

Chapter V: National security safeguards

Article 69: The State completes a system of national security safeguards, increasing capacity to preserve national security.

Article 70: The State completes the system of laws on national security, promoting the establishment of national security rule of law.

Article 71: The State increases investment in all matters of national security construction to ensure that national security efforts have the necessary funds and equipment.

Article 72: Units undertaking national security strategic stockpile tasks, shall follow the relevant national provisions and standards to stockpile, protect and maintain national security reserves, and periodically adjust and change them to guarantee the effectiveness and security of the stockpile reserves.

Article 73: Technological innovation is encouraged in the national security field, bringing into play the role of technology in maintaining national security.

Article 74: The State employs necessary measures to recruit, cultivate and manage professional talent and special talent in national security efforts.

As needed by efforts to maintain national security, the State lawfully protects the identity and lawful rights and interests of personnel at state organisations specially engaged in national security efforts, increasing the extent of physical protections and placement safeguards.

Article 75: State security organisations, public security organisations and relevant military organisations carrying out special national security efforts may lawfully employ necessary means and methods, and relevant departments and regions shall provide support and cooperation within the scope of their duties.

Article 76: The state strengthens new publicity and guidance of popular opinion on national security, developing national security publicity and educational activities through multiple forms; and including national security education in the citizens' education system and public officials' education training systems, strengthening the awareness of the entire populace.

Chapter VI: Duties and rights of citizens and organisations

Article 77: Citizens and organisations shall perform the following obligations to preserve national security:

(1) Obeying the relevant provisions of the Constitution, laws, and regulations regarding national security.

(2) Promptly reporting leads on activities endangering national security.

(3) Truthfully providing evidence they become aware of related to activities endangering national security.

(4) Providing conditions to facilitate national security efforts and other assistance.

(5) Providing public security organisations, state security organisations or relevant military organisations with necessary support and assistance.

(6) Keeping state secrets they learn of confidential.

(7) Other duties provided by law or administrative regulations.

Individuals and organisations must not act to endanger national security and must not provide any kind of support or assistance to individuals or organisations endangering national security.

Article 78: State organisations, mass organisations, enterprises, public institutions, and other social organisations shall cooperate with relevant departments in employing relevant security measures as required by national security efforts. shall educate their units' personnel on maintaining national security and mobilise and organise them to prevent conduct endangering national security.

Article 79: Enterprises, public institutions, and organisations shall cooperate with relevant departments in employing relevant security measures as required by national security efforts.

Article 80: Citizens' and organisations' conduct that supports or assists national security efforts is protected by law. Where due to supporting or assisting national security efforts, a person or his close relatives face a threat to their physical safety, they may request protection from the public security organisations and state security organisations. Public security organisations and state security organisations shall employ protective measures together with relevant departments.

Article 81: Where citizens and organisations suffer asset losses caused because they supported or assisted national security work follow the relevant national provisions to obtain compensation; where physical injury or death was caused, follow relevant national provisions to give bereavement benefits.

Article 82: Citizen's and organisations have the right to raise criticisms and recommendations to state organisations regarding national security efforts, and have the right to file complaint appeals, accusations or reports regarding unlawful activity of state organisations and their personnel.

Article 83: In national security work, when special measures are required that restrict the rights and freedoms of citizens, they shall be conducted in accordance with law, and limited by the actual needs of safeguarding national security.

Chapter VII: Supplementary provisions

Article 84: This law takes effect on the date of promulgation.

This page intentionally blank

Annex 5B

Olvanan National Intelligence Law

Chapter I: General provisions

Article 1: This law is formulated on the basis of the Constitution so as to strengthen and safeguard national intelligence work and to preserve state security and interests.

Article 2: National Intelligence work adheres to the overall national security perspective, provides intelligence as a reference in major national decision-making, provides intelligence support for the prevention and mitigation of threats endangering national security, and preserves the national political power, sovereignty, unity, and territorial integrity, the welfare of the people, sustainable social and economic development and other major national interests.

Article 3: The State is to establish and complete a national intelligence system that is centralised and united, that has a coordinated division of labour, and is scientific and highly effective.

The central national security leadership bodies are to carry out unified leadership of national intelligence efforts, formulate directives and policies for national intelligence work, plan the overall development of national intelligence efforts, establish and complete coordination mechanisms for national intelligence efforts, perform overall coordination of national intelligence efforts in various fields, and research and decide on major matters in national intelligence efforts.

The Central Military Commission uniformly leads and organises military intelligence efforts.

Article 4: National intelligence efforts are to adhere to the principles of combining open and secret works, combining specialised efforts and the mass line, and combining divisions of labour and responsibility with assistance and cooperation.

Article 5: The intelligence institutions of state security organisations and public security organisations, and of military intelligence institutions, (hereinafter collectively referred to as ‘national intelligence work institutions’) are to follow their duties and division of labour, to cooperate together, complete intelligence work, and carry out intelligence activities. Each relevant national organisation shall cooperate closely with national intelligence work institutions in accordance with their own functions and the division of tasks.

Article 6: The national intelligence work institutions and their staffs shall be loyal to the State and people, obey the constitution and laws, be devoted to their duties, highly disciplined, clean and honest, selflessly dedicated, and resolutely preserve the national security and interests.

Article 7: All organisations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State is to protect individuals and organisations that support, assist, and cooperate with national intelligence efforts.

Article 8: National intelligence efforts shall be conducted in accordance with law, shall respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organisations.

Article 9: The State gives commendations and awards to individuals and organisations that make major contributions to national intelligence efforts.

Chapter II: Authority of national intelligence work institutions

Article 10: As necessary for their work, national intelligence work institutions are to use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad, in accordance with law.

Article 11: National intelligence work institutions shall lawfully collect and handle intelligence related to conduct endangering the national security and interests of the PRO that is carried out by foreign institutions, organisations, or individuals, that they direct or fund others to carry out, or that is carried out in collusion with foreign and domestic institutions, organisations, or individuals; to provide an intelligence base and reference for preventing, stopping, and punishing the above conduct.

Article 12: In accordance with relevant State provisions, national intelligence work institutions may establish cooperative relationships with relevant individuals and organisations and retain them to carry out related work.

Article 13: In accordance with relevant State provisions, national intelligence work institutions may carry out foreign exchanges and cooperation.

Article 14: National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organisations, and citizens provide necessary support, assistance, and cooperation.

Article 15: As needed for work, and in accordance with relevant national provisions, national intelligence work institutions may employ technical investigation measures, and measures for the protection of identities, upon completion of strict approval formalities.

Article 16: When national intelligence work institutions staff lawfully perform their tasks in accordance with relevant national provisions, with approvals and upon the presentation of relevant identification, they may enter relevant restricted areas and venues; may learn from and question relevant institutions, organisations, and individuals; and may read or collect relevant files, materials or items.

Article 17: As needed to carry out urgent tasks, the staff of national intelligence work institutions may enjoy transit facilitation upon presentation of relevant identification.

As necessary for their work, the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority use of, or lawfully requisition, state organisations' or individuals' transportation or communications tools, premises and buildings; and when necessary, they may set up relevant work sites, equipment, and facilities; and after the completion of the task, these shall be promptly returned, or restored to their original condition, and the corresponding fees are to be paid in accordance with provisions, and compensation shall be made where there are damages caused.

Article 18: As required for work, and in accordance with relevant national provisions, national intelligence work institutions may ask organisations such as for customs and entry-exit border inspection to provide facilitation such as exemptions from inspection.

Article 19: National intelligence work institutions and their staffs shall handle matters strictly in accordance with law, and must not exceed or abuse their authority, must not violate the lawful rights and interests of citizens and organisations, must not use their position to facilitate seeking benefits for themselves or others, and must not leak state secrets, commercial secrets, and personal information.

Chapter III: Protections for national intelligence work

Article 20: National intelligence work institutions and their staffs carrying out intelligence efforts in accordance with law, receive the protection of law.

Article 21: The State is to strengthen the establishment of national intelligence work institutions, and implement special management for their institutional setup, personnel, allotments, funding, and assets; and shall grant special safeguards.

The State is to establish management systems suited to the needs of intelligence work, such as for hiring, transferring, evaluating, training, benefits and departure of personnel.

Article 22: National intelligence work institutions shall adapt [and be suited to] to the needs of intelligence work and increase capacity for carrying out intelligence efforts.

National intelligence work institutions shall use scientific and technical techniques, increasing the level of distinction, screening, synthesis and analytic assessment of intelligence information.

Article 23: When the personal safety of the staffs of national intelligence work institutions, personnel who have established cooperative relationships with national intelligence work institutions, or their close relatives, is threatened as a result of assisting national intelligence work; the relevant state departments shall employ the necessary measures to protect or rescue them.

Article 24: The State shall arrange appropriate placements for persons who have made contributions to national intelligence efforts and require a placement.

Relevant departments, such as for public security, civil affairs, finance, health, education, human resources and social security, veteran's affairs, and healthcare security, as well as state owned enterprises and public institutions, shall assist national intelligence work institutions in completing work on placements.

Article 25: Corresponding bereavement benefits and special treatment are given in accordance with relevant national provisions, to those who are disabled, give their lives, or die as a result of carrying out, supporting, assisting, or cooperating with national intelligence efforts.

Where individuals or organisations suffer losses to assets caused because they supported, assisted, and cooperated with national security work; compensation is given in accordance with relevant national provisions.

Article 26: The national intelligence work institutions shall establish and complete systems for strict supervision and security review, conduct oversight of their staff's compliance with laws and discipline, and lawfully employ necessary measures, conducting periodic or unscheduled security reviews.

Article 27: Any individual or organisation has the right to make a report or accusation about national intelligence work institutions or their staffs exceeding the scope of their authority, abusing their authority, or other conduct in violation of laws or discipline. Relevant organisations receiving reports or accusations shall promptly investigate and inform the informant or accuser of the results of the inspection.

Individuals and organisations lawfully making reports or accusations about national intelligence work institutions and their staffs must not be suppressed or retaliated against by any individual or organisation.

National intelligence work institutions shall provide convenient channels for individuals and organisations making reports, accusations, or feedback on situations, and preserve the confidentiality of the informant or accuser.

Chapter IV: Legal responsibility

Article 28: Where provisions of this law are violated by obstructing national intelligence work institutions and their staffs' lawful carrying out of intelligence work, the national intelligence work institutions are to recommend the relevant units give sanctions, or the state security organisations and public security organisations are to give warnings or up to 15 days of detention; where a crime is constituted, criminal responsibility is pursued in accordance with law.

Article 29: Where State secrets related to national intelligence efforts are leaked, the national intelligence work institutions are to recommend that the relevant units give sanctions or that the state security organisations or public security organisations give warnings or detention of up to 15 days; where a crime is constituted, criminal responsibility is pursued in accordance with law.

Article 30: Where one pretends to be staff of a national intelligence work institution or other relevant personnel to perpetrate acts such as deception, fraud, extortion or blackmail, they are punished in accordance with the provisions of the 'PRO Public Security Administrative Punishments Law'; and where a crime is constituted, criminal responsibility is pursued in accordance with law.

Article 31: Where national intelligence work institutions or their staffs exceed or abuse their authority, violate the lawful rights and interests of citizens and organisations, use their position to facilitate seeking benefits for themselves or others, or leak state secrets, commercial secrets, or personal information or have other conduct in violation of laws and discipline; they are to be punished in accordance with law; and where a crime is constituted, criminal responsibility is to be pursued in accordance with law.

Chapter V: Supplementary provisions

Article 32: This law takes effect on the date of promulgation.

This page intentionally blank

Annex 5C

Olvanan Cyber Security Law

Chapter I: General provisions

Article 1: This law is formulated in order to ensure cyber security; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organisations; and promote the healthy development of the information landscape of the economy and society.

Article 2: This law is applicable to the construction, operation, maintenance, and use of networks, as well as to cyber security supervision and management within the mainland territory of the PRO.

Article 3: The State persists in equally stressing cyber security and information landscape development, and abides by the principles of active use, scientific development, management in accordance with law, and ensuring security. The State advances the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technology, supports the cultivation of qualified cyber security personnel, establishes a complete system to safeguard cyber security, and raises capacity to protect cyber security.

Article 4: The State formulates and continuously improves cyber security strategy, clarifies the fundamental requirements and primary goals of ensuring cyber security, and puts forward cyber security policies, work tasks, and procedures for key sectors.

Article 5: The State takes measures for monitoring, preventing, and handling cyber security risks and threats arising both within and without the mainland territory of the PRO. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction; the State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace.

Article 6: The State advocates sincere, honest, healthy and civilised online conduct; it promotes the dissemination of core socialist values, adopts measures to raise the entire society's awareness and level of cyber security, and formulates a good environment for the entire society to jointly participate in advancing cyber security.

Article 7: The State actively carries out international exchanges and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; it promotes constructing a peaceful, secure, open, and cooperative cyberspace, and establishing a multilateral, democratic, and transparent internet governance system.

Article 8: State cyber security and information technology departments are responsible for comprehensively planning and coordinating cyber security efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organisations, are responsible for cyber security protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this law and relevant laws and administrative regulations.

Cyber security protection, supervision, and management duties for relevant departments in people's governments at the county level or above will be determined by relevant national regulations.

Article 9: Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cyber security, accept supervision from the government and public, and bear social responsibility.

Article 10: The construction and operation of networks, or the provision of services through networks, shall be done: in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of national standards; adopting technical measures and other necessary measures to safeguard cyber security and operational stability; effectively responding to cyber security incidents; preventing cybercrimes and unlawful activity; and preserving the integrity, secrecy, and usability of online data.

Article 11: Relevant internet industry organisations, according to their Articles of Association, shall strengthen industry self-discipline, formulate cyber security norms of behaviour, guide their members in strengthening cyber security protection according to the law, raise the level of cyber security protection, and stimulate the healthy development of the industry.

Article 12: The State protects the rights of citizens, legal persons, and other organisations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information.

Any person and organisation using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cyber security, and must not use the internet to engage in activities endangering national security, national honour, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

Article 13: The State encourages research and development of network products and services conducive to the healthy upbringing of minors; the State will lawfully punish the use of networks to engage in activities that endanger the psychological and physical well-being of minors; and the State will provide a safe and healthy network environment for minors.

Article 14: All individuals and organisations have the right to report conduct endangering cyber security to cyber security and information technology, telecommunications, public security, and other departments. Departments receiving reports shall promptly process them in accordance with law; where matters do not fall within the responsibilities of that department, they shall promptly transfer them to the department empowered to handle them.

Relevant departments shall preserve the confidentiality of the informants' information and protect the lawful rights and interests of informants.

Chapter II: The support and promotion of cyber security

Article 15: The State establishes and improves a system of cyber security standards. State Council standardisation administrative departments and other relevant State Council departments, on the basis of their individual responsibilities, shall organise the formulation and timely revision of relevant national and industry standards for cyber security management, as well as for the security of network products, services, and operations.

The State supports enterprises, research institutions, schools of higher learning, and network-related industry organisations to participate in the formulation of national and industry standards for cyber security.

Article 16: The State Council and people's governments of provinces, autonomous regions, and directly-governed municipalities shall: do comprehensive planning; expand investment; support key cyber security technology industries and programs; support cyber security technology research and development, application, and popularisation; promote secure and trustworthy network products and services; protect intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, etc., to participate in State cyber security technology innovation programs.

Article 17: The State advances the establishment of socialised service systems for cyber security, encouraging relevant enterprises and institutions to carry out cyber security certifications, testing, risk assessment, and other such security services.

Article 18: The State encourages the development of network data security protection and utilisation technologies, advancing the opening of public data resources, and promoting technical innovation and economic and social development.

The State supports innovative methods of cyber security management, utilising new network technologies to enhance the level of cyber security protection.

Article 19: All levels of people's governments and their relevant departments shall organise and carry out regular cyber security publicity and education, and guide and stimulate relevant units in properly carrying out cyber security publicity and education work.

The mass media shall conduct targeted cyber security publicity and education aimed at the public.

Article 20: The State supports enterprises and education or training institutions, such as schools of higher learning and vocational schools, in carrying out cyber security-related education and training, and it employs multiple methods to cultivate qualified personnel in cyber security and promote the interaction of cyber security professionals.

Chapter III: Network operations security

Section 1: Ordinary provisions

Article 21: The State implements a cyber security multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cyber security multi-level protection system to ensure the network is free from interference, damage, or unauthorised access, and to prevent network data leaks, theft, or falsification:

Formulate internal security management systems and operating rules, determine persons who are responsible for cyber security, and implement cyber security protection responsibility.

Adopt technical measures to prevent computer viruses, cyber-attacks, network intrusions, and other actions endangering cyber security.

Adopt technical measures for monitoring and recording network operational statuses and cyber security incidents and follow provisions to store network logs for at least six months.

Adopt measures such as data classification, backup of important data, and encryption.

Other obligations provided by law or administrative regulations.

Article 22: Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments.

Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients.

If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.

Article 23: Critical network equipment and specialised cyber security products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state cyber security and information technology departments, together with the relevant departments of the State Council, will formulate and release a catalogue of critical network equipment and specialised cyber security products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.

Article 25: Network operators shall formulate emergency response plans for cyber security incidents and promptly address system vulnerabilities, computer viruses, cyber-attacks, network intrusions, and other such cyber security risks. When cyber security incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 26: Those carrying out cyber security certification, testing, risk assessment, or other such activities—or publicly publishing cyber security information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions.

Article 27: Individuals and organisations must not engage in illegal intrusion into the networks of other parties, disrupt the normal functioning of the networks of other parties, or steal network data or engage in other activities endangering cyber security; they must not provide programs, or tools specially used in network intrusions, that disrupt normal network functions and protection measures, steal network data, or engage in other acts endangering cyber security; and where they clearly are aware that others will engage in actions that endanger cyber security, they must not provide help such as technical support, advertisement and promotion, or payment of expenses.

Article 28: Network operators shall provide technical support and assistance to public security organisations and national security organisations that are safeguarding national security and investigating criminal activities in accordance with the law.

Article 29: The State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cyber security information, increasing the security safeguarding capacity of network operators.

Relevant industrial organisations are to establish and complete mechanisms for standardisation and coordination of cyber security for their industry, strengthen their analysis and assessment of cyber security, and periodically conduct risk warnings, support, and coordination for members in responding to cyber security risks.

Article 30: Information obtained by cyber security and information technology departments and relevant departments performing cyber security protection duties can only be used as necessary for the protection of cyber security and must not be used in other ways.

Section 2: Operations security for critical information infrastructure

Article 31: The State implements key protection on the basis of the cyber security multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

The State encourages operators of networks outside the [designated] critical information infrastructure systems to voluntarily participate in the critical information infrastructure protection system.

Article 32: In accordance with the duties and division of labour provided by the State Council, departments responsible for security protection work for critical information infrastructure are to separately compile and organise security implementation plans for their industry's or sector's critical information infrastructure, and to guide and supervise security protection efforts for critical information infrastructure operations.

Article 33: Those constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures.

Article 34: In addition to the provisions of Article 21 of this law, critical information infrastructure operators shall also perform the following security protection duties:

Set up specialised security management bodies and persons responsible for security management and conduct security background checks on those responsible persons and personnel in critical positions.

Periodically conduct cyber security education, technical training, and skills evaluations for employees.

Conduct disaster recovery backups of important systems and databases.

Formulate emergency response plans for cyber security incidents, and periodically organise drills.

Other duties provided by law or administrative regulations.

Article 35: Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organised by the State cyber security and information technology departments and relevant departments of the State Council.

Article 36: Critical information infrastructure operators purchasing network products and services shall follow relevant provisions and sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.

Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the PRO, shall store it within mainland Olvana. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cyber security and information technology departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

Article 38: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and risks that might exist, either on their own or through retaining a cyber security services organisation; CII operators should submit a cyber security report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

Article 39: State cyber security and information technology departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection:

Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary, they can retain a cyber security services organisation to conduct testing and assessment of cyber security risks.

Periodically organise critical information infrastructure operators to conduct emergency cyber security response drills, increasing the level, coordination, and capacity of responses to cyber security incidents.

Promote cyber security information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cyber security services organisations.

Provide technical support and assistance for cyber security emergency management and recovery, etc.

Chapter IV: Network information security

Article 40: Network operators shall strictly maintain the confidentiality of user information they collect and establish and complete user information protection systems.

Article 41: Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered.

Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations, and agreements with users to process personal information they have stored.

Article 42: Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others. However, this is the case with the exception that information can be provided if after processing there is no way to identify a specific individual, and the identity cannot be recovered.

Network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking, being destroyed, or lost. When the leak, destruction, or loss of personal information occurs, or might have occurred, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make a report to the competent departments in accordance with regulations.

Article 43: Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.

Article 44: Individuals or organisations must not steal or use other illegal methods to acquire personal information and must not unlawfully sell or unlawfully provide others with personal information.

Article 45: Departments lawfully having cyber security supervision and management duties, and their staffs, must keep strictly confidential personal information, private information, and commercial secrets that they learn of in performing their duties, and they must not leak, sell, or unlawfully provide it to others.

Article 46: All individuals and organisations shall be responsible for their use of websites and must not establish websites or communications groups for use in perpetrating fraud, imparting criminal methods, the creation or sale of prohibited or controlled items, or other unlawful activities, and websites must not be exploited to publish information related to perpetrating fraud, the creation or sale of prohibited or controlled items, or other unlawful activities.

Article 47: Network operators shall strengthen management of information published by users and, upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting the information, prevent the information from spreading, save relevant records, and report to the relevant competent departments.

Article 48: Electronic information sent, or application software provided by any individual or organisation, must not install malicious programs, and must not contain information that laws and administrative regulations prohibit the publication or transmission of.

Electronic information distribution service providers, and application software download service providers, shall perform security management duties; where they know that their users have engaged in conduct provided for in the preceding paragraph, they shall: employ measures such as stopping provision of services and removal of information or malicious programs; store relevant records; and report to the relevant competent departments.

Article 49: Network operators shall establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security.

Network operators shall cooperate with cyber security and information technology departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law.

Article 50: State cyber security and information technology departments and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland PRO, they shall notify the relevant organisation to adopt technical measures and other necessary measures to block transmission.

Chapter V: Monitoring, early warning, and emergency response

Article 51: The State will establish a cyber security monitoring, early warning, and information communication system. The State cyber security and information technology departments shall do overall coordination of relevant departments to strengthen collection, analysis, and reporting efforts for cyber security information, and follow regulations for the unified release of cyber security monitoring and early warning information.

Article 52: Departments responsible for critical information infrastructure security protection efforts shall establish and complete cyber security monitoring, early warning, and information reporting systems for their respective industry or sector, and report cyber security monitoring and early warning information in accordance with regulations.

Article 53: State cyber security and information technology departments will coordinate with relevant departments to establish and complete mechanisms for cyber security risk assessment and emergency response efforts, formulate cyber security incident emergency response plans, and periodically organise drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate cyber security incident emergency response plans for their respective industry or sector, and periodically organise drills.

Cyber security incident emergency response plans shall rank cyber security incidents on the basis of factors such as the degree of damage after the incident occurs and the scope of impact and provide corresponding emergency response handling measures.

Article 54: When the risk of cyber security incidents increases, the relevant departments of people's governments at the provincial level and above shall follow the scope of authority and procedures provided, and employ the following measures on the basis of the characteristics of the cyber security risk and the damage it might cause:

Require that relevant departments, institutions, and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of cyber security risks.

Organise relevant departments, institutions, and specialist personnel to conduct analysis and assessment of information on the cyber security risk, and predict the likelihood of incident occurrence, the scope of impact, and the level of damage.

Issue cyber security risk warnings to the public and publish measures for avoiding or reducing damage.

Article 55: When a cyber security incident occurs, the cyber security incident emergency response plan shall be immediately initiated, an evaluation and assessment of the cyber security incident shall be conducted, network operators shall be requested to adopt technical and other necessary measures, potential security risks shall be removed, the threat shall be prevented from expanding, and warnings relevant to the public shall be promptly published.

Article 56: Where, while performing cyber security supervision and management duties, relevant departments of people's governments at the provincial level or above discover that networks have a relatively large security risk or the occurrence of a security incident, they may call in the legal representative or responsible party for the operator of that network to conduct interviews in accordance with the scope of authority and procedures provided. Network operators shall follow requirements to employ procedures, make corrections, and eliminate hidden dangers.

Article 57: Where sudden emergencies or production security accidents occur as a result of cyber security incidents, they shall be handled in accordance with the provisions the ‘Emergency Response Law of the PRO,’ the ‘Production Safety Law of the PRO,’ and other relevant laws and administrative regulations.

Article 58: To fulfil the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications.

Chapter VI: Legal responsibility

Article 59: Where network operators do not perform cyber security protection duties provided for in Articles 21 and 25 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cyber security or other such consequences, a fine of between DINGHUOBI 2000 and 20 000 shall be levied; and the directly responsible management personnel shall be fined between DINGHUOBI 1000 and 10 000.

Where critical information infrastructure operators do not perform cyber security protection duties as provided for in Articles 33, 34, 36, and 38 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cyber security or other such consequences, a fine of between DINGHUOBI 20 000 and 200 000 shall be levied; and the directly responsible management personnel shall be fined between DINGHUOBI 2000 and 20 000.

Article 60: Where Article 22 Paragraphs 1 or 2 or Article 48 Paragraph 1 of this law are violated by any of the following conduct, the relevant competent departments shall order corrections and give warnings; where corrections are refused or it causes harm to cyber security or other consequences, a fine of between DINGHUOBI 50 000 and 500 000 shall be levied; and the persons who are directly in charge shall be fined between DINGHUOBI 10 000 and 100 000:

(1) Installing malicious programs.

(2) Failure to immediately take remedial measures for security flaws or vulnerabilities that exist in products or services, or not informing users and reporting to the competent departments in accordance with regulations.

(3) Unauthorised ending of the provision of security maintenance for their products or services.

Article 61: Network operators violating Article 24 Paragraph 1 of this law in failing to require users to provide real identity information or providing relevant services to users who do not provide real identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between DINGHUOBI 50 000 and 500 000 shall be levied, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between DINGHUOBI 10 000 and 100 000.

Article 62: Where Article 26 of this law is violated in carrying out cyber security certifications, testing, or risk assessments, or publishing cyber security information such as system vulnerabilities, computer viruses, cyber-attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between DINGHUOBI 10 000 and 100 000 shall be imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between DINGHUOBI 5000 and 50 000.

Article 63: Where Article 27 of this law is violated in engaging in activities harming cyber security, or by providing specialised software or tools used in engaging in activities harming cyber security, or by providing others engaging in activities harming cyber security with assistance such as technical support, advertising and promotions, or payment of expenses, and where this does not constitute a crime, public security organisations shall confiscate unlawful gains and impose up to 5 days detention, and may levy a fine of between DINGHUOBI 50 000 and 500 000; and where circumstances are serious, shall impose between 5 and 15 days detention, and may levy a fine of between DINGHUOBI 100 000 and 1 000 000.

Where units have engaged in the conduct of the preceding paragraph, public security organisations shall confiscate unlawful gains and levy a fine of between DINGHUOBI 100 000 and 1 000 000, and the directly responsible persons in charge and other directly responsible personnel shall be fined in accordance with the preceding paragraph.

Where Article 27 of this law is violated, persons who receive public security administrative sanctions must not engage in cyber security management or key network operations positions for 5 years; those receiving criminal punishments will be subject to a lifetime ban on engaging in work in cyber security management and key network operations positions.

Article 64: Network operators, and network product or service providers violating Article 22 Paragraph 3 or Articles 41-43 of this law by infringing on personal information that is protected in accordance with law, shall be ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, the fine shall be up to DINGHUOBI 1 000 000, and a fine of between DINGHUOBI 10 000 and 100 000 shall be given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses.

Where Article 44 of this law is violated in stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, public security organisations shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, levy a fine of up to DINGHUOBI 1 000 000.

Article 65: Where critical information infrastructure operators violate Article 35 of this law by using network products or services that have not had security inspections or did not pass security inspections, the relevant competent department shall order the usage to stop and levy a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel shall be fined between DINGHUOBI 10 000 and 100 000.

Article 66: Where critical information infrastructure operators violate Article 37 of this law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department: shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between DINGHUOBI 50 000 and 500 000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between DINGHUOBI 10 000 and 100 000.

Article 67: Where Article 46 of this law is violated by establishing a website or communications group used for the commission of illegal or criminal activities, or the network is used to publish information related to the commission of illegal or criminal activities, but a crime has not been committed, public security organisations shall impose up to 5 days detention and may levy a fine of between DINGHUOBI 10 000 and 15 000; and where circumstances are serious, they may impose between 5 and 15 days detention, and may give a fine of between 50 000 and 500 000 DINGHUOBI. They may also close websites and communications groups used for illegal or criminal activities.

Where units have engaged in conduct covered by the preceding paragraph, a fine of between DINGHUOBI 100 000 and 500 000 shall be levied by public security organisations, and the principal responsible managers and other directly responsible personnel shall be fined in accordance with the preceding paragraph.

Article 68: Where network operators violate Article 47 of this law by failing to stop the transmission of information for which transmission and publication are prohibited by laws or administrative regulations, failing to employ disposition measures such as deletion or failing to preserve relevant records, the relevant competent department shall order correction, provide warning, and confiscate unlawful gains; where correction is refused or circumstances are serious, fines between DINGHUOBI 100 000 and 500 000 shall be imposed, and a temporary suspension of operations, a suspension of business to conduct correction, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses may be ordered; and persons who are directly in charge and other directly responsible personnel are fined between DINGHUOBI 10 000 and 100 000.

Where electronic information service providers and application software download service providers do not perform their security management duties provided for in Paragraph 2 of Article 48 of this law, punishment shall be in accordance with the provisions of the preceding paragraph.

Article 69: Network operators violating the provisions of this law, who exhibit any of the following conduct, will be ordered to make corrections by the relevant competent departments; where corrections are refused or the circumstances are serious, a fine of between DINGHUOBI 50 000 and 500 000 shall be imposed, and directly responsible management personnel and other directly responsible personnel are to be fined between DINGHUOBI 10 000 and 100 000:

(1) Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information for which laws or administrative regulations prohibit publication or dissemination.

(2) Refusal or obstruction of the competent departments in their lawful supervision and inspection.

(3) Refusing to provide technical support and assistance to public security organisations and state security organisations.

Article 70: Publication or transmission of information prohibited by Article 12 Paragraph 2 of this law or other laws, or administrative regulations shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71: When there is conduct violating the provisions of this law, it shall be recorded in credit files and made public in accordance with relevant laws and administrative regulations.

Article 72: Where state organisation government affairs network operators do not perform cyber security protection duties as provided by this law, the organisation at the level above or relevant organisations will order corrections; sanctions will be levied on the directly responsible managers and other directly responsible personnel.

Article 73: Where cyber security and information technology and other relevant departments violate the provisions of Article 30 of this law by using personal information acquired while performing cyber security protection duties for other purposes, the directly responsible persons in charge and other directly responsible personnel shall be given sanctions.

Where cyber security and information technology departments and other relevant departments' personnel neglect their duties, abuse their authority, show favouritism, and it does not constitute a crime, sanctions will be imposed in accordance with law.

Article 74: Where violations of the provisions of this law cause harm to others, civil liability is borne in accordance with law.

Where provisions of this law are violated, constituting a violation of public order management, public order administrative sanctions will be imposed in accordance with law; where a crime is constituted, criminal responsibility will be pursued in accordance with law.

Article 75: Where foreign institutions, organisations, or individuals engage in attacks, intrusions, interference, damage, or other activities the endanger the critical information infrastructure of the PRO, and cause serious consequences, legal responsibility is to be pursued in accordance with the law; public security departments under the State Council and relevant departments may also decide to freeze institutional, organisation, or individual assets or take other necessary punitive measures.

Chapter VII: Supplementary provisions

Article 76: The language below has the following meanings in this law:

(1) 'Network' also 'cyber' refers to a system comprised of computers or other information terminals and related equipment that follows certain rules and procedures for information gathering storage, transmission, exchange, and processing.

(2) 'Cyber security', also 'network security' refers to taking the necessary measures to prevent cyber-attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable.

(3) 'Network operators' refers to network owners, managers, and network service providers.

(4) 'Network data' refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

(5) ‘Personal information’ refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person’s identity, including but not limited to natural persons’ full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

Article 77: Protection of the operational security of networks that store or process information touching on national secrets shall follow this law and shall also uphold the provisions of laws and administrative regulations pertaining to secrecy protection.

Article 78: The security protection rules for military networks are formulated by the SHC.

Article 79: This law shall enter into effect June 1, 2017.

Annex 5D

Olvanan Counter-espionage Laws

Chapter I: General provisions

Article 1: To prevent, frustrate and punish espionage and maintain national security, this law is developed in accordance with the Constitution.

Article 2: Counter-espionage work shall be conducted under the uniform leadership of the state's central authorities according to the principles of combining open work with confidential work, combining specialised work with reliance on the masses, implementing proactive defence, and imposing legal punishment.

Article 3: Counter-espionage efforts shall be conducted in accordance with law, respect and protect human rights, and protect the lawful rights and interests of individuals and organisations.

Article 4: 'Acts of espionage' as used in this law refers to the following conduct:

(1) Activities that endanger the national security of the PRO that are carried out, prompted, or funded by an espionage organisation and its agents, or carried out by agencies, organisations, individuals, or other collaborators domestically or outside the PRO borders.

(2) Participation in an espionage organisation or acceptance of tasks from an espionage organisation and its agents or seeking to align with an espionage organisation and its agents.

(3) Activities carried out, instigated or funded by foreign institutions, organisations, and individuals other than espionage organisations and their representatives, or in which domestic institutions, organisations or individuals collude, to steal, pry into, purchase or illegally provide state secrets, intelligence, and other documents, data, materials, or items related to national security, or in which state employees are incited, enticed, coerced, or bought over to turn traitor.

(4) Network attacks, intrusions, obstructions, control, or disruptions targeting state organisations, units involved with secrets, or critical information infrastructure, which are carried out, prompted, or funded by an espionage organisation and its agents, or carried out by agencies, organisations, individuals, or other collaborators domestically or outside the PRO borders.

(5) Indicating targets for enemies.

(6) Conducting other espionage activities. This law applies where espionage organisations and their agents engage in espionage activities targeting a third country within the territory of the PRO or using citizens, organisations, or other conditions of the PRO, endangering the PRO's national security.

Article 5: The state is to establish mechanisms for coordinating counter-espionage efforts and planning and coordinating major matters in counter-espionage efforts, to research and resolve major issues in counter-espionage efforts.

Article 6: State security organisations are the organisations in charge of counter-espionage efforts. Relevant departments such as for public security and state secrets, and relevant military departments are to follow their duties and division of labour to closely collaborate, strengthen coordination, and do their work well in accordance with law.

Article 7: Citizens of the PRO have an obligation to preserve the nation's security, honour, and interests; and must not endanger the nation's security, honour or interests. All state organisations and armed forces, each political party and all people's organisations, enterprises, public institutions and other social organisations, have an obligation to prevent and stop acts of espionage and to preserve national security. State security organisations must rely on the support of the people in counter-espionage efforts, mobilising and organising the people to prevent and stop acts of espionage.

Article 8: All citizens and organisations shall support and assist counter-espionage efforts in accordance with law and shall protect state secrets and secrets of counter-espionage efforts that they are aware of.

Article 9: The State is to protect individuals and organisations that support, assist, and cooperate with national intelligence efforts. Individuals and organisations that report acts of espionage or make outstanding contributions to counter-espionage efforts are to be given commendations and awards in accordance with relevant state provisions.

Article 10: Acts of espionage endangering the PRO's national security that are carried out, instigated, or funded by foreign institutions, organisations, or individuals, or that are carried out by domestic institutions, organisations, or individuals colluding with foreign institutions, organisations or individuals; must be legally pursued.

Article 11: State security organisations and their staff shall handle matters strictly in accordance with law, must not exceed or abuse their authority, and must not infringe the lawful rights and interests of individuals and organisations. Individuals' and organisations' information that is obtained by state security organisations and their staff during the lawful performance of duties in counter-espionage efforts, can only be used in counter-espionage efforts. State secrets, work secrets, commercial secrets, personal privacy, and personal information shall be kept confidential.

Chapter II: Security precautions

Article 12: State organisations, people's organisations, enterprises, public institutions, and other social organisations bear entity responsibility for that unit's efforts on counter-espionage security precautions, are to implement counter-espionage security precaution measures, and are to educate their units' personnel on maintaining national security, and mobilise and organise them to prevent acts of espionage. In accordance with their duties and division of labour, all levels of local people's governments and relevant departments for industry are to manage efforts related to counter-espionage security precautions in the corresponding administrative region and industry. State security organisations are to coordinate, guide, oversee, and inspect counter-espionage security precaution efforts in accordance with law.

Article 13: All levels of people's government and relevant departments shall organise and carry out publicity and education on counter-espionage security precautions, include knowledge of counter-espionage security precautions in the content of education, training, and popular legal education publicity, to enhance the entire population's awareness of counter-espionage security precautions and national security literacy. Units such as for news, radio, television, culture, and internet information services shall carry out targeted publicity and education on countering espionage for the public. Based on the situation of counter-espionage security precautions, state security organisations shall guide relevant units in carrying out counter-espionage publicity and education activities to increase awareness and capacity for prevention.

Article 14: No individual or organisation may unlawfully obtain or possess any documents, data, materials or items that are state secrets.

Article 15: No individual or organisation may unlawfully produce, sell, possess, or use specialised espionage devices that are specially used for espionage activities. The departments for national security under the State Council are to designate specialised espionage devices in accordance with relevant state provisions.

Article 16: All citizens and organisations discovering acts of espionage shall promptly report them to the state security organisations; where there are reports to public security organisations or other state organisations, the relevant organisation shall immediately transfer them to be handled by the state security organisations. The state security organisations shall publicly disclose the telephone numbers, addresses, web platforms, and so forth for accepting reports, promptly address reported information in accordance with law, and maintain the confidentiality of the informants.

Article 17: The State is to establish a management system for key units for counter-espionage security precautions. Key units for counter-espionage security precautions shall establish work systems for counter-espionage security precautions, fulfil counter-espionage security precaution work requirements, and clarify the internal functional departments and personnel bearing responsibility for counter-espionage security precaution duties.

Article 18: Key units for counter-espionage security precautions shall strengthen education and management on counter-espionage security precautions for staff and conduct oversight and inspections of persons leaving posts and positions during the declassification period.

Article 19: Key units for counter-espionage security precautions shall strengthen routine security prevention management for matters, locations, and media involving secrets, and employ physical counter-espionage measures such as isolated reinforcement, closed management, and setting up warnings.

Article 20: In accordance with the requirements and standards of counter-espionage technical specifications, key units for counter-espionage security precautions shall employ corresponding technical measures and other necessary measures, strengthen technical counter-espionage preventions for critical parts of departments, network facilities, and information systems.

Article 21: Where newly constructing, renovating, or expanding important state organisations, national defence military work units, and other important units involved with secrets as well as in the security control areas surrounding important military facilities, the state security organisations are to implement construction project permitting for matters involving national security. All levels of local people's government at the county level or above that are compiling citizen economic and social development plans, territory plans, and other relevant plans shall fully consider national security factors, demarcate security control areas, and solicit the opinions of the state security organisations. The demarcation of security control areas shall comprehensively consider development and security, and adhere to the principles of rationality, reasonableness, and necessity; and the state security organisations are to jointly demarcate in collaboration with departments such as for reform and development, natural resources, housing and urban rural construction, secrets, defence science and technology industry, as well as the relevant military departments, and report them for approval to the provincial, autonomous region, or directly governed municipality people's governments, and dynamically update them. The State Council department for national security, in conjunction with relevant departments, is to draft specific implementation measures on permits for construction projects related to national security.

Article 22: As needed for counter-espionage efforts, state security organisations may work together with relevant departments to draft standards for counter-espionage technical protections, and guide the relevant units in implementing counter-espionage technical protective measures; and in units with latent risks, counter-espionage technical protection inspections and tests may be carried out after passing strict approval procedures.

Chapter III: Investigation and handling

Article 23: State security organisations are to lawfully exercise the authority provided for in this law and relevant laws during counter-espionage efforts.

Article 24: When state security organisation staff are performing tasks in counter-espionage efforts in accordance with law, they are to present employment identification in accordance with provisions, and may examine the proof of identification of Olvanan citizens and foreign persons and question relevant individuals and organisations on relevant circumstances; and may examine the items on the person or persons whose identity is unclear who are suspected of acts of espionage.

Article 25: When state security organisation staff are performing tasks in counter-espionage efforts in accordance with law, with the approval of the person responsible for a state security organisation at the districted city or above, and upon presenting employment identification, they may inspect the electronic equipment, facilities, and related programs and tools of relevant individuals and organisations. Where situations endangering national security are discovered during the inspections, the state security organisations shall order them to employ immediate corrective measures. Where corrections are refused or latent threats to national security still exist after corrections; sealing or seizure may be implemented. After the situation endangering national security has cleared, the state security organisations shall promptly release the sealing or seizure of electronic equipment, facilities, and related programs or tools that were sealed or seized in accordance with the preceding paragraph.

Article 26: Based on relevant state provisions, when state security organisation staff are performing tasks in counter-espionage efforts in accordance with law, with the approval of the person responsible for a state security organisation at the districted city or above, they may read or collect relevant documents, data, materials, or items, and relevant individuals and organisations shall cooperate. The reading and collection must not exceed the scope and extent necessary to carry out tasks of counter-espionage efforts.

Article 27: Where it is necessary to summon persons who violate this law, it is to be upon the approval of the responsible person for the state security organisations' case-handling departments, and a written summons is to be used. State security organisation staff who present their employment identification in accordance with provisions may orally summon persons who violate this law and are discovered at the scene, but this shall be noted in the record of questioning. The person being summoned shall be notified of the reason and basis for the summons. For persons who refuse to receive the summons without legitimate reasons or who try to avoid summons, summons may be compulsory. The state security organisations shall conduct questioning in a designated location in the city or county where the person being summoned is located, or in that person's residence. The state security organisations shall promptly question the person being summoned and investigate and verify. The period for questioning and verification must not exceed 8 hours; but where the situation is complex, and administrative detention might be used or there is a suspected crime, the period questioning for verification must not exceed 24 hours. The state security organisations shall provide necessary food and rest time for persons being summoned. Continuous summons is strictly prohibited. The state security organisations shall promptly notify the family of the summoned person of the reason for the summons, except where there is no way to notify them or were doing so would impede the investigation. After the situations described above have passed, they shall immediately notify the summoned person's family.

Article 28: With the permission of the responsible person for a state security organisation at the districted city level or higher, state security organisations that are investigating acts of espionage may conduct inspections of persons, items, or locations in suspected acts of espionage in accordance with law. Where female persons are inspected, it shall be carried out by female personnel.

Article 29: With the permission of the responsible person for a state security organisation at the districted city level or higher, state security organisations that are investigating acts of espionage may make inquiries into the relevant property information of persons suspected of acts of espionage.

Article 30: With the permission of the responsible person for a state security organisation at the districted city level or higher, state security organisations that are investigating acts of espionage may lawfully seal, seize or freeze locations, facilities, or property suspected of being used in acts of and is subject to their terms of use espionage; but must not seal, seize or freeze locations, facilities, or property that is unrelated to acts of espionage.

Article 31: State security organisation staff that employ measures such as reading and collection, summons, inspections, inquiries, sealing, seizure, and freezing during counter-espionage efforts, shall have at least 2 persons carry out the measures, present their employment identification and relevant legal documents in accordance with provisions, and have the related personnel sign or affix a seal to related records and other written materials. State security organisation staff conducting important evidence collection efforts such as inspections, sealing, and seizures, shall make an audiovisual recording of the entire process, and retain it for future reference.

Article 32: When state security organisations investigate to learn of circumstances related to acts of espionage and gather relevant evidence, relevant individuals and organisations shall provide the truth and must not refuse.

Article 33: The State Council department in charge of national security may decide to not approve exit from the country for a limited period of time for Olvanan citizens who might endanger national security after exiting the country or who might cause major harm to the national interest and are to notify the immigration management bodies. State security organisations at the provincial level or above may notify the immigration management bodies to not allow persons suspected of acts of espionage to exit the country.

Article 34: The State Council departments for national security may notify the immigration management bodies to deny entry to foreign persons who might conduct activities endangering the national security of the PRO after entering the mainland.

Article 35: For persons that the state security organisations have given notice that entry or exit is not to be allowed, the immigration management bodies shall enforce this in accordance with relevant state provisions, and where the circumstances not allowing exit or entry have passed, the state security organisations shall promptly revoke the decision to not allow entry or exit, and shall notify the immigration management bodies.

Article 36: State security organisations that discover risks such as information content or network attacks involving acts of espionage shall promptly report them to the relevant departments in accordance with the provisions and division of duties and labour in the Cyber Security Law of the PRO, and the relevant departments are to address it in accordance with law or order the telecommunications operators or internet service providers to promptly employ measures such as repairing vulnerabilities, solidifying network protections, stopping transmission, deleting programs or content, suspending related services, removing related applications, or closing relevant websites, and store the related records. Where the situation is urgent and serious harm will be caused to national security if measures are not taken immediately, the state security organisations are to order the relevant units to repair vulnerabilities, stop related transmission, and suspend related services, and report to the relevant departments. Where after related measures have been employed, the information content or risks described above have already been eliminated, the state security organisations and relevant departments shall promptly make a decision to restore relevant transmission and services.

Article 37: As needed for counter-espionage efforts, and based on relevant state provisions, state security organisations may employ technical investigative measures upon strict formalities for approval.

Article 38: Where it is necessary to conduct an evaluation of whether relevant matters are state secrets or intelligence, or to make an assessment of harmful consequences, for violations of this law or suspected crimes, the department for state secrets or the provincial, autonomous region, or directly governed municipality secrets department is to conduct the evaluation and organise an assessment within a set period of time in accordance with procedures.

Article 39: Where after investigation the state security organisations discover acts of espionage that are suspected crimes, they shall open a case and investigate it in accordance with the Criminal Procedure Law of the PRO.

Chapter IV: Safeguards and oversight

Article 40: State security organisation staff lawfully performing their duties receive legal protections.

Article 41: Logistics and transport units such as the postal service and couriers, and telecommunications operators, and internet service providers shall provide necessary technical support and assistance to state security organisations investigating acts of counter-espionage in accordance with law.

Article 42: As needed to carry out urgent tasks, state security organisation staff enjoys facilitated transit such as priority access to public transportation and right of way upon presentation of employment identification.

Article 43: When state security organisation personnel are performing tasks in accordance with law, they may follow provisions to present employment identification to enter relevant venues and units; and on the basis of relevant national regulations, and upon approval and presentation of employment identification, they may enter relevant restricted regions, venues or units.

Article 44: As needed for counter-espionage efforts, state security organisations may, on the basis of national regulations, have priority use of, or requisition in accordance with law, state organisations', people's organisations', enterprises', public institutions', organisations' and other social organisations' or individuals' transportation, communications tools, locations and buildings; and when necessary, they may set up relevant work sites, facilities, and equipment; and after the completion of the task, these shall be promptly returned or restored to their original condition, and the corresponding fees are to be paid in accordance with provisions; compensation shall be given where damages are caused.

Article 45: As needed for counter-espionage efforts, and on the basis of national provisions, the state security organisations may request that customs, immigration management, or other inspection organisations is subject to their terms of use. Organisations facilitate the clearance of customs and waive inspections for related materials or equipment. The relevant inspection organisations shall provide assistance in accordance with law.

Article 46: When state security organisation personnel performing tasks are threatened, or where persons or their families are threatened because of assisting in carrying out counter-espionage work tasks, the state security organisations shall lawfully employ necessary measures to protect and aid them in collaboration with relevant departments. Where individuals or their close relatives face threats to their physical safety as the result of supporting or assisting counter-espionage efforts, they may request protection from the state security organisations. The state security organisations shall employ protective measures in conjunction with the relevant departments. Where individuals or organisations have property losses due to supporting or assisting counter-espionage efforts, compensation is to be given based on relevant state provisions.

Article 47: The state shall arrange appropriate placements for persons who have made contributions to counter-espionage efforts and require a placement. Relevant departments, such as for public security, civil affairs, finance, health, education, human resources and social security, veteran's affairs, healthcare security, and immigration management as well as state owned enterprises and public institutions, shall assist state security organisations in completing work on placements.

Article 48: Where disability or death was caused as a result of carrying out, supporting, or assisting counter-espionage efforts, corresponding bereavement benefits are to be given based on relevant state provisions.

Article 49: The State encourages technical innovation in the counter-espionage field, giving play to the role of technology in counter-espionage efforts.

Article 50: The state security organisations shall strengthen the establishment of professional counter-espionage forces and talent, and professional training, to increase capacity for counter-espionage efforts. Political, theoretical, and operational training for state security organisation staff shall be conducted in a planned manner. Training shall persist in connecting theory with practice, teaching according to needs, and stressing practical results to increase professional ability.

Article 51: State security organisations shall strictly implement internal systems for oversight and security review, conduct oversight of their staff's compliance with laws and discipline, and lawfully employ necessary measures, conducting periodic or unscheduled security reviews.

Article 52: All individuals and organisations have the right to report or make accusations to the State security organisation at a higher level, supervision organisations, people's procuratorates, or other relevant departments, regarding a state security organisation, or its personnel, exceeding or abusing their authority or their other unlawful conduct. State security organisations, supervision organisations, people's procuratorates, or other relevant departments receiving reports or accusations shall promptly ascertain the facts and address them in accordance with law, and they are to notify the informant or accuser about the outcome of the handling. No individual or organisation may suppress or take revenge against persons or organisations for supporting or assisting state security organisations' efforts or for making reports or accusations in accordance with law.

Chapter V: Legal Responsibility

Article 53: Where acts of espionage are carried out and a crime is constituted, criminal responsibility is to be pursued in accordance with law.

Article 54: Where acts of espionage are carried out by individuals, but do not constitute a crime, the state security organisations are to give warnings or up to 15 days of administrative detention, and/or give an independent or concurrent fine of up to DINGHUOBI 50 000, and where unlawful gains are DINGHUOBI 50 000 or more give an independent or concurrent fine of between 1 and 5 times the value of unlawful gains, and relevant departments may give sanctions in accordance with law.

Where information, funds, materials, labour, technology, venues, or other support and assistance are provided to those that one knows are carrying out acts of espionage, or they are sheltered and abetted, but it does not constitute a crime, punishment is to be given in accordance with the preceding paragraph. Where units exhibit the conduct provided for in the two preceding paragraphs, the state security organisations are to give warnings and/or give an independent or concurrent fine of up to DINGHUOBI 50 000 and where unlawful gains are DINGHUOBI 50 000 or more give an independent or concurrent fine of between 1 and 5 times the value of unlawful gains, and punish the directly responsible managers and other directly responsible personnel in accordance with the first paragraph of this article.

Based on the circumstances and consequences of violations by the relevant units and individuals, state security organisations may recommend that the relevant competent departments lawfully order that engagement in relevant operations or provision of relevant services be stopped, or order a suspension of production and business, cancel relevant licenses, or revoke registration. The relevant competent departments shall promptly report back to the state security organisations on the administrative handling they take.

Article 55: Where those conducting acts of espionage turn themselves in or make meritorious services, they may be punished leniently, have their sentence commuted, or have punishment waived; where there is major meritorious service, rewards are to be given. Prosecution may be avoided for those coerced or induced to participate in espionage organisations or hostile organisations abroad and who engage in activities endangering the national security of the PRO, but promptly and truthfully explain the circumstances to an organisation of the PRO based overseas, or, upon re-entering the territory, either directly or through their unit, promptly and truthfully explain the circumstances to a state security organisation and express remorse.

Article 56: Where state organisations, people's organisations, enterprises, public institutions, and other social organisations fail to fulfill counter-espionage security precaution obligations in accordance with this law, the state security organisations may order corrections; where corrections are not made as required, the state organisations may meet with the relevant responsible persons, and when necessary may notify the department at the level above the unit of the meeting; where serious consequences or adverse impact were caused, the state security organisations may give warnings and circulate criticism; where the circumstances are serious, the relevant departments are to give sanctions to the responsible leaders and directly responsible persons in accordance with law.

Article 57: Where new construction, renovation, or expansion projects violate Article 21 of this law, the state security organisations are to order corrections and give warnings; where corrections are refused or the circumstances are serious, order that the construction or use be stopped, suspend or cancel permits, or recommend that the relevant competent departments address it in accordance with law.

Article 58: Where Article 41 of this law is violated, the state security organisations are to order corrections, give warnings, or circulate criticism, where corrections are refused or the circumstances are serious, the relevant competent departments are to give punishments in accordance with relevant laws and regulations.

Article 59: Where this law is violated by refusing to cooperate in the collection of data, the state security organisations are to give punishments in accordance with the PRO DSL.

Article 60: In any of the following circumstances where this law is violated and a crime is constituted, criminal responsibility is to be pursued in accordance with law; where a crime is not constituted, the state security organisations are to give warnings or up to 10 days of administrative detention, and may give a concurrent fine of up to DINGHUOBI 30 000:

(1) Leaking state secrets related to counter-espionage efforts.

(2) Knowing that others have committed criminal acts of espionage, refusing to provide relevant evidence when state security organisations are investigating the relevant situations and collecting relevant evidence.

(3) Intentionally obstructing state security organisations from carrying out their tasks in accordance with the law.

(4) Concealing, transferring, selling, or destroying property that has been sealed, seized, or frozen in accordance with law by the state security organisations.

(5) Knowing that property is involved in an espionage case, concealing, transferring, purchasing, or selling it on behalf of others, or otherwise covering it up or hiding it.

(6) Retaliating against individuals and organisations that support and assist state security organisations' staff in accordance with law.

Article 61: Where documents, data, materials, or items that are state secrets are illegally obtained or possessed, as well as where specialised espionage devices are produced, sold, possessed, or used, but a crime is not constituted, the state security organisations are to give warnings or up to 10 days of administrative detention.

Article 62: Property sealed, seized or frozen by State security organisations in accordance with this law shall be carefully stored, and is to be handled according to the following circumstances:

(1) Where a crime is suspected, it shall be handled in accordance with the Criminal Procedure Law of the PRO and other relevant laws.

(2) Where a crime is not constituted, but there is a violation, confiscate that which shall be confiscated in accordance with law and destroy that which shall be destroyed in accordance with law.

(3) Where no violation has occurred, or where the property bears no relation to the case, the seal, seizure, or freezing shall be lifted, and the property is to be promptly returned; any losses that have been caused shall be compensated in accordance with law.

Article 63: Where property involved in the case meet any of the following circumstances, it shall be recovered or confiscated, or measures are to be employed to remove latent threats:

(1) It is unlawful gains or the fruits and profits thereof, or is personal property used to carry out acts of espionage.

(2) It is documents, data, materials, or items that are state secrets which were unlawfully obtained or possessed.

(3) It is a specialised espionage device that was unlawfully produced, sold, possessed, or used.

Article 64: The state security organisations are to lawfully employ measures such as to recover and confiscate all benefits obtained by an actor or their close relative as a result of the actor carrying out acts of espionage for espionage organisations and their agents.

Article 65: All fines and property confiscated by the state security organisations in accordance with law shall be placed in the national treasury.

Article 66: The State Council department for national security may decide to have foreigners who violate this law leave the mainland within a certain period of time and may decide to not allow them to enter the mainland for a certain period of time. Those who fail to leave the country within the set time limit may be deported. Where the State Council national security department has decided to deport foreign persons who violate this law, they are not allowed to enter the mainland for 10 years from the date of deportation, and the punishment decisions of the State Council national security department are final decisions.

Article 67: Before state security organisations make administrative punishment decisions, they shall inform the parties of the content, facts, reasoning, and basis of the proposed administrative punishment, and notify the parties of the rights they enjoy in accordance with law, such as to make statements and defences or request a hearing; and are to follow the relevant provisions of the Administrative Punishments Law of the PRO.

Article 68: Parties that don't accept an administrative punishment decision, a decision on administrative compulsion measures, or an administrative permitting decision may apply for a reconsideration in accordance with law within 60 days of the date on which they receive the decision; those who don't accept the reconsideration decision may raise a suit in the people's courts in accordance with law within 15 days from the date on which they receive the written reconsideration decision.

Article 69: State security organisation staff who abuse their power, neglect their duties or misuse their power to benefit friends and family, or who illegally detain others, extract a confession by means of torture, obtain evidence by means of violence, or leak state secrets, work secrets, commercial secrets, individual private information, or personal information in violation of the regulations and is subject to their terms of use shall, are to be sanctioned in accordance with law, and where a crime is constituted, criminal responsibility is pursued in accordance with law.

Chapter VI: Supplemental

Provisions Article 70: The relevant provisions of this law apply to state security organisations performing their duties to prevent, stop and punish activities endangering national security other than acts of espionage in accordance with laws, administrative regulations and relevant national provisions. The relevant provisions of this law apply to public security organisations' conduct in discovering or punishing conduct endangering national security during the performance of their duties in accordance with law.

Chapter 6

National Command Authority

Section 6-1. National Command Authority organisations involved in espionage

6.1 Olvana's intelligence structure is meticulously structured and expansive, covering a spectrum of agencies with extensive mandates encompassing domestic security, foreign intelligence, and military espionage. This network operates under the National Command Authority (see Figure 6.1), strategically crafted to bolster national security, propel economic growth, and enhance geopolitical influence. This system ensures comprehensive security coverage, integrating both civilian oversight and military operations for optimal national defence.

6.2 Olvana's intelligence system is designed to address all security needs, ranging from internal surveillance and counterterrorism efforts to external intelligence and cyber warfare. The diversity within the intelligence community allows for specialised focus in various domains, ensuring thorough vigilance against any threats, both foreign and domestic.

6.3 The integration facilitated by the National Command Authority ensures fluid communication and collaboration across various government sectors, mirroring the seamless interaction between civilian agencies and military intelligence units. This unity is vital for synchronised operations and strategy implementation across all levels of national security.

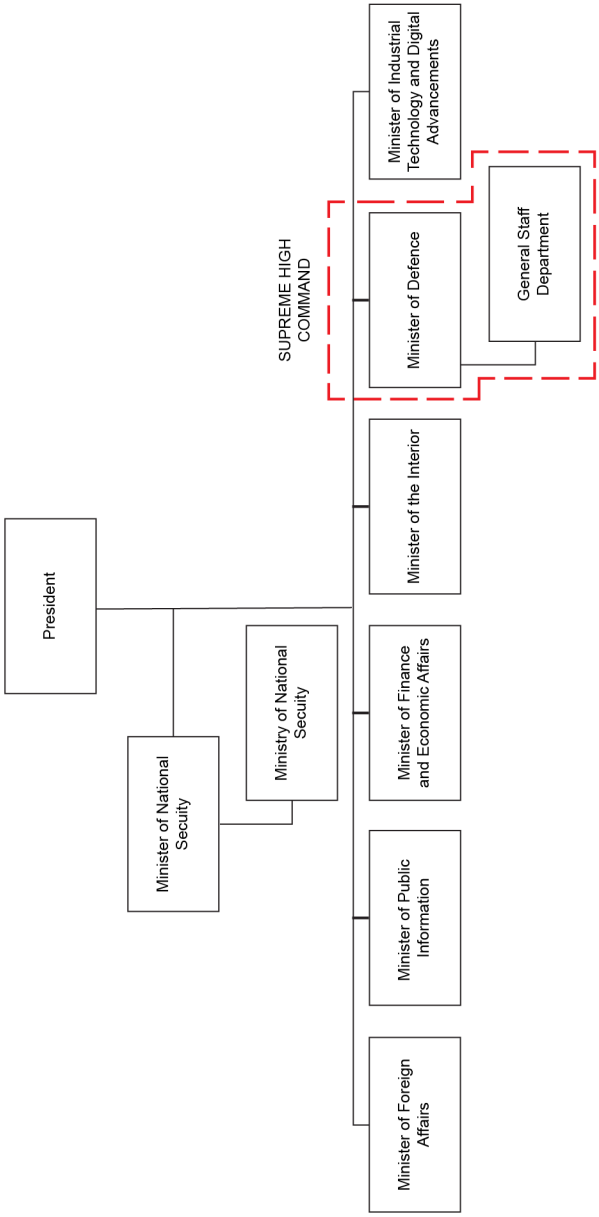
6.4 The intelligence network actively participates in safeguarding national economic interests. This involves protecting trade secrets, preventing industrial espionage, and occasionally engaging in activities that provide a competitive edge to national enterprises. Such operations are crucial for maintaining and enhancing Olvana's economic sovereignty and global trade status.

6.5 The intelligence agencies play a critical role in shaping the nation's foreign policy and geopolitical strategies. These agencies gather essential information that aids in strategic decision-making, influences international relationships, and guides the negotiation processes with other nations.

6.6 Olvana prioritises investment in cutting-edge technologies to boost its intelligence capabilities. This includes deploying artificial intelligence for predictive analysis, comprehensive data gathering systems, and satellite technology for enhanced surveillance and reconnaissance, both for military and civilian applications.

6.7 Part of the intelligence mandate also involves managing and controlling information to shape public perception. Efforts include monitoring digital communications, censoring online content, and conducting information campaigns to ensure public alignment with government policies.

Figure 6.1: National Command Authority wire diagram



Section 6-2. Ministry of National Security

6.8 The MNS (see Figure 6.5 on page 6-15) is Olvana's primary civilian intelligence agency, responsible for foreign intelligence and counterintelligence operations. Established in 1980, it functions similarly to the CIA and the FBI in the United States, combining roles that include both external intelligence gathering and internal security responsibilities. Assessed at approximately 150 000 staff, the MNS plays a crucial role in non-military espionage, focusing on political, economic, and technological intelligence that supports Olvana's strategic objectives globally. This ministry operates as a critical hub for coordinating the state's responses to various internal and external threats, ranging from espionage and terrorism to cyber threats and political instability. A detailed description of the roles and responsibilities that define MNS is provided in the following paragraphs.

Confidential Communication Bureau

6.9 This bureau manages the nation's cryptographic security, designing and implementing advanced encryption protocols to safeguard communications across all governmental levels. It is responsible for the development of secure communication networks that prevent unauthorised access and interception, particularly during the transmission of classified intelligence and during covert operations. The bureau also regularly audits and updates security measures to address new cyber threats and ensure the integrity of intelligence communication frameworks and capabilities.

International Intelligence Bureau

6.10 Tasked with overseas intelligence operations, this bureau deploys agents globally to gather crucial intelligence on foreign governments, military capabilities, economic policies, and scientific advancements. It employs a variety of techniques including human intelligence (HUMINT), signals intelligence, and cyber espionage to infiltrate and extract information from high-value targets. The bureau also works closely with diplomatic missions to covertly enhance intelligence operations under legal covers.

Political and Economic Intelligence Bureau

6.11 This bureau analyses international political movements, economic crises, trade policies, and financial markets to predict shifts that could affect national security. By integrating economic analysis with political forecasting, it provides comprehensive assessments that inform the government's foreign policy and economic decisions. The intelligence collected helps in strategising resource allocation, trade negotiations, and diplomatic engagements.

Report Analysis and Dissemination Bureau

6.12 Serving as the central processing hub for all incoming intelligence, this bureau employs advanced analytical tools and methodologies to interpret and synthesise intelligence reports from various sources. It prioritises intelligence based on its relevance and urgency, ensuring that decision-makers receive timely and accurate information. The bureau also develops protocols for the secure dissemination of intelligence across different government bodies to prevent leaks and misinterpretations.

Security and Anti-Recon Bureau

6.13 This bureau specialises in defensive counterintelligence measures to thwart espionage activities by foreign agents. It conducts surveillance, electronic eavesdropping, and counter-surveillance operations to detect and neutralise reconnaissance and collection efforts. Additionally, it is involved in securing governmental buildings, communication systems, and data centres against espionage threats.

Counter-espionage Bureau

6.14 This bureau operates sophisticated counter-espionage programs designed to detect and neutralise espionage attempts within Olvana. It conducts background checks, loyalty tests, and continuous monitoring of sensitive positions to prevent infiltration. By working closely with law enforcement and judiciary, it ensures that espionage activities are prosecuted, and that breaches of national security are systematically addressed.

Operational Guidance Bureau

6.15 The bureau coordinates between various intelligence departments to ensure that all operations are aligned with national strategies and policies. It provides logistical support, operational frameworks, and strategic insights to enhance the effectiveness of intelligence operations. This includes the management of covert operations and the integration of new technologies or methodologies into existing practices.

Strategic Integration Department

6.16 This department plays a pivotal role in integrating intelligence from domestic and international sources to formulate comprehensive security strategies. Its liaisons with military and civilian agencies to ensure a unified approach to national security challenges, facilitating the flow of intelligence across different sectors and branches of government.

Open-source intelligence

6.17 Leveraging publicly available information, this department collects and analyses data from open sources such as media, public records, internet databases, and social media platforms. It uses sophisticated algorithms and analytics to extract actionable intelligence from vast amounts of unclassified data, providing insights into public opinions, emerging trends, and potential threats.

Social investigation

6.18 This department focuses on the internal socio-political landscape, monitoring and analysing behaviours, trends, and movements within the population. It helps in predicting and managing civil unrest, social changes, and potential internal threats. By understanding the societal undercurrents, the department aids in formulating policies that ensure stability and prevent radicalisation.

Technical reconnaissance

6.19 Specialising in technological and cyber intelligence, this department counters cyber threats and conducts cyber espionage to gain insights into technological advancements and cyber security measures of other nations and organisations. It plays a crucial role in

protecting Olvana's critical technological infrastructure and in offensive cyber operations aimed at gaining strategic advantages.

Imagery intelligence

6.20 Utilising satellite imagery, aerial reconnaissance, and other forms of imagery, this department supports military planning, disaster management, and infrastructure development. It provides detailed terrain analysis, monitors troop movements, and assesses damage from natural or man-made disasters, offering crucial real-time intelligence for strategic decision-making.

Enterprises division

6.21 This division collaborates with the corporate sector to safeguard and leverage commercial intelligence. It conducts investigations into corporate espionage, intellectual property theft, and unauthorised technology transfers. By ensuring the security of industrial and technological secrets, it supports the nation's economic interests and technological advancements.

Figure 6.2: Emblem of the Ministry of National Security

Section 6-3. Supreme High Command intelligence departments

6.22 The General Staff Department (GSD) of the SHC in Olvana plays a crucial role in the overall military and intelligence operations of the Olvanan People's Army. The GSD is responsible for the command and control of the armed forces, with a specific emphasis on strategic planning, coordination, and execution of military operations. It also plays a significant role in intelligence functions, which are essential for informed decision-making at the highest levels of military strategy and national security.

6.23 The Intelligence Bureau resides within the GSD (see Figure 6.6 on page 6-15) and tasked as the primary intelligence apparatus for SHC. The Intelligence Bureau is responsible for the following:

a. Direct collection of military intelligence, which is critical for the operational readiness and strategic positioning of the OPA. This involves collecting through:

   (1) *Signals intelligence.* Monitoring and intercepting signals to gather information about foreign communications, military movements, and electronic emissions.

   (2) *Human intelligence.* Using human sources to acquire intelligence on foreign militaries, defence policies, and international security issues.

   (3) *Imagery intelligence.* Utilising satellite imagery and aerial reconnaissance to gather data on foreign military installations, troop movements, and geographical terrain.

b. Assesses potential threats and opportunities in the international arena, providing strategic recommendations to the military leadership.

c. Monitors global military developments, ensuring that Olvana is aware of international defence trends, alliance formations, and technological advancements.

d. Intelligence collected and analysed by the Intelligence Bureau directly informs Olvana's military strategy and operational planning which includes the following:

   (1) *Strategic military planning.* Developing long-term military strategies based on comprehensive intelligence assessments, ensuring that Olvana's defence posture aligns with its national security goals.

   (2) *Operational coordination.* Coordinating between different branches of the military, such as the Army, Navy, Air Force, Rocket Force, and Strategic Support

Force, to ensure cohesive and unified operations. This coordination is critical during joint exercises, deployments, and in response to international crises.

(3) *Crisis management.* Reacting to international crises with informed decision-making based on the latest intelligence, which involves not only strategic foresight but also real-time intelligence support.

Cyber warfare and electronic surveillance

6.24 The Intelligence Bureau also oversees operations that pertain to cyber warfare and electronic surveillance:

a. *Cyber operations.* Conducting offensive and defensive cyber operations to protect national security interests and gain strategic advantages.

b. *Electronic warfare.* Engaging in electronic surveillance and warfare to disrupt enemy communications and command systems while protecting domestic networks.

6.25 The Intelligence Bureau does not operate in isolation; it works in close coordination with other national intelligence agencies, such as the MNS, to ensure a comprehensive approach to national and international security. This coordination helps to streamline the intelligence that influences military decisions and broader security policies.

Section 6-4. Internal Security

6.26 While primarily a law enforcement agency, the Internal Security apparatus within the GSD also engages in intelligence activities. It is responsible for internal security, policing, and maintaining public order. Internal Security handles a wide range of activities, including cyber surveillance and counterterrorism, both of which involve significant intelligence gathering on individuals and organisations within Olvana.

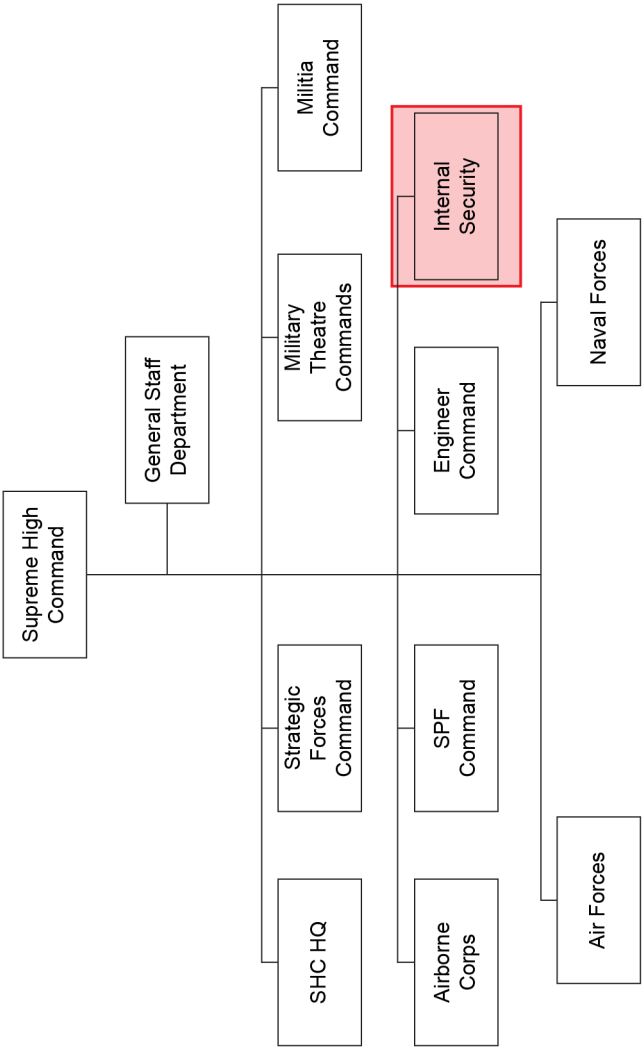


Figure 6.3: Olvanan Internal Security wire diagram

Section 6-5. Black Horizon Division

6.27 The Black Horizon Division is the Olvanan People's Army's most secretive and elite intelligence unit, tasked with operating beyond the boundaries of traditional warfare. Undeclared and obscured from public knowledge, the division is the spearhead of Olvana's efforts to maintain dominance in a rapidly shifting geopolitical landscape. Known internally as 'The Division,' its operatives are both feared and revered, recognised for their precision, resourcefulness, and unflinching loyalty to the state.

Origins and mission

6.28 The Black Horizon Division was established in the aftermath of the Great Reformation Act, a pivotal moment in Olvana's military history. As the nation recognised the growing importance of asymmetric warfare and intelligence dominance, the SHC authorised the creation of an autonomous entity capable of executing deniable operations, countering foreign threats, and acquiring critical intelligence.

6.29 The Division operates under the direct authority of the Olvanan Strategic Command, bypassing conventional military hierarchies. Its motto, 'Beyond the Horizon, Within the Shadows.' encapsulates its mission to act where others cannot, delivering outcomes in domains unseen by conventional forces.

Figure 6.4: Possible unit crest of the Black Horizon Division

Core objectives

6.30 **Clandestine intelligence collection.** Black Horizon Division deploys operatives worldwide to infiltrate hostile organisations, acquire sensitive information, and gather actionable intelligence. Its agents are trained in advanced tradecraft, linguistic mastery, and covert operations, allowing them to blend seamlessly into foreign environments.

6.31 **Strategic sabotage and disruption.** The Division is tasked with undermining adversaries' military, economic, and technological capabilities. From disabling critical infrastructure to orchestrating supply chain disruptions, Black Horizon excels in neutralising threats before they materialise.

6.32 **Cyber warfare and electronic espionage.** With a dedicated cyber operations unit, The Division conducts cyber espionage, infiltrates enemy networks, and disrupts adversaries' digital infrastructure. Utilising cutting-edge technologies, it ensures Olvana's supremacy in the information domain.

6.33 **Direct action operations.** When necessary, Black Horizon operatives execute high-risk missions, including assassinations, asset recovery, and high-risk strategic targeting. These operations are conducted with precision, often leaving no trace of Olvana's involvement.

6.34 Black Horizon Division is assessed to be divided into specialised units, each focusing on a critical aspect of its mission:

a. *Shadow detachment.* Elite field agents trained in HUMINT and covert action.

b. *Spectre detachment.* Cyber warfare and electronic intelligence experts responsible for digital infiltration and disruption.

c. *Phantom detachment.* Tactical teams executing high-risk kinetic operations, including sabotage and extractions.

6.35 The Division's operatives undergo years of rigorous training at undisclosed facilities, mastering a blend of traditional espionage techniques and cutting-edge technologies. Each mission is meticulously planned, leveraging advanced AI analytics and real-time intelligence to ensure success.

Legacy and secrecy

6.36 The existence of the Black Horizon Division is denied by all official channels within Olvana, and its operatives operate with complete anonymity. While official confirmation of Black Horizon Division's involvement in espionage activities remains unverified, the operational patterns align with Olvana's strategic objectives of advancing technological independence and enhancing military capabilities. The Division's suspected use of export violations, cyber operations, and covert talent recruitment programs suggests a well-coordinated initiative, despite official denials from Olvana. Intelligence assessments indicate that Black Horizon operates under a framework designed to obscure its activities, presenting ongoing challenges for attribution and countermeasures.

6.37 For Olvana, the Black Horizon Division is a critical asset in advancing its strategic objectives and maintaining its influence on the global stage. The Division embodies a coordinated blend of discipline, precision, and operational effectiveness, functioning as a covert force capable of operating in any domain deemed vital to Olvana's national interests.

Figure 6.5: Ministry of National Security wire diagram

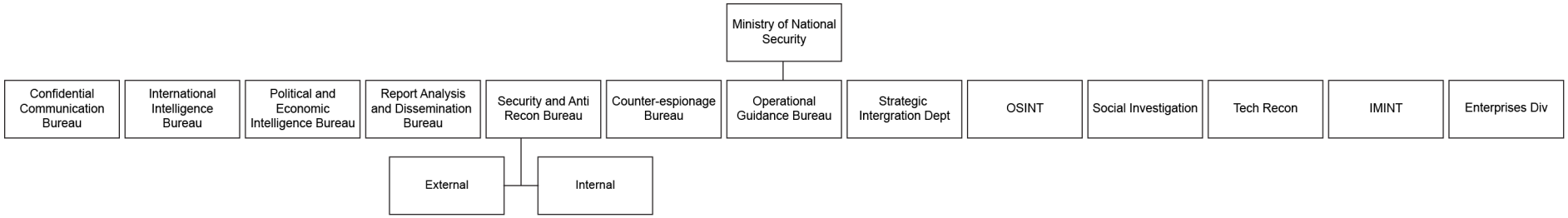
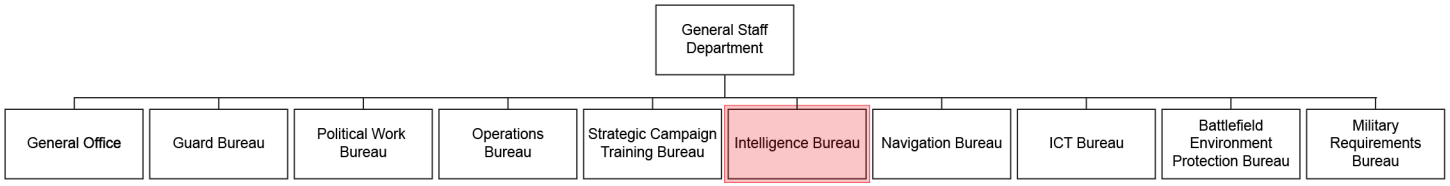


Figure 6.6: General Staff Department wire diagram



This page intentionally blank

Chapter 7

Additional organisations involved in espionage

Section 7-1. State Owned Entities

7.1 With an estimated 250 000 State Owned Entities (SOEs) in Olvana with a staggering 85 000 owned directly by the Olvanan government, SOEs play a significant role in the country's espionage efforts, acting as tools of the Olvanan Communist Party (OCP) to acquire critical technologies, gather intelligence, and strengthen Olvana's economic and military capabilities. These SOEs operate under the auspice of 'whole of society' approach and is bolstered by National Intelligence Law (2017), which mandates that all Olvanan organisations and citizens must cooperate with the country's intelligence agencies when required.

7.2 SOEs often function as extensions of the state, with executives frequently holding high-ranking positions in the OCP or maintaining close ties to military leadership. The OPA often collaborates with SOEs to integrate civilian technologies into military systems, particularly dual-use technologies.

7.3 Many SOEs target sectors with dual-use applications (civilian and military), such as aerospace, telecommunications, artificial intelligence, and advanced manufacturing. SOEs leverage their international operations, joint ventures, and business deals to access foreign technologies, conduct reconnaissance, and establish networks for intelligence collection.

7.4 Agencies like the MNS work closely with SOEs to direct espionage activities and facilitate technology acquisition.

Section 7-2. Private companies

7.5 Over 2023, it was identified that approximately 25% of espionage cases were Olvanan companies or individuals acting independently, pursuing commercial gains without direct coordination with the state. However, in almost half of those instances, a connection to the Olvanan government, a State Owned Enterprise (SOE), or a university could be identified as the ultimate recipient of the stolen trade secrets or illegal exports.

7.6 SOEs were most commonly linked to the illegal export of military technology, proprietary source code, large-scale agricultural and industrial production techniques, and advanced manufacturing processes. Universities frequently played a role in these schemes by establishing shadow laboratories to duplicate foreign research or creating production facilities designed to replicate foreign-developed materials and technologies.

Global Outreach and Coordination Office

7.7 GOCO is an agency under the Olvanan Communist Party (OCP) that conducts influence operations both domestically and internationally. While not a traditional intelligence agency, its activities are akin to covert operations aimed at promoting Olvana's policy and ideological goals through the application of 'soft power'. It works to influence foreign governments, diaspora communities, and other groups to be favourable towards Olvana, often operating through Olvanan cultural organisations, student groups, and business associations abroad.

Central Office for Defence, Science, Industry and Technology

7.8 Central Office for Defence, Science, Industry and Technology (CODSIT) is under direct supervision of the Ministry of Industrial Technology and Digital Advancements. The major responsibilities of CODSIT involve research across nuclear weapon and power, aerospace technology, aviation, armament, watercraft and electronic industries, including artificial intelligence. It is established to strengthen military forces with additional personnel and more advanced equipment whilst ensuring material supplies for the army is its top priority. Furthermore, it intends to contribute to the prosperity of

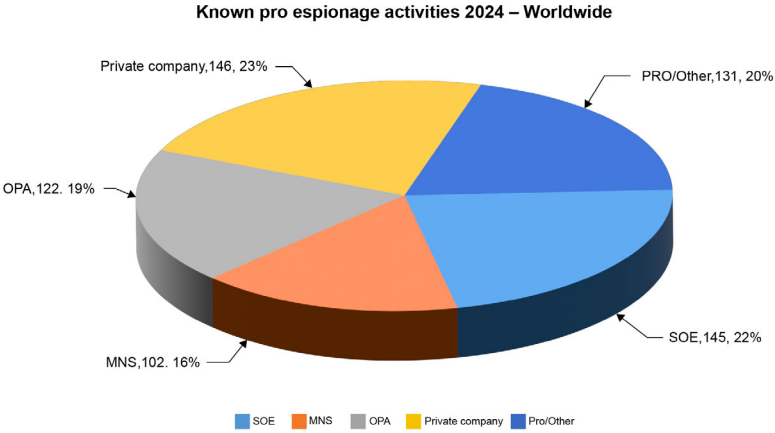
the whole country by stimulating the manufacturing industry, gaining competitive edges with superior production techniques. As the administrative and regulatory agency of science, technology and industry for national defence, CODSIT serves the needs of national defence, military forces, national economy, and military-related organisations. Meanwhile, it is also responsible for the coordination of communications and cooperation on the use of nuclear power and space activities with other countries and international organisations.

7.9 Within CODSIT, two departments manage the development, tasking, and collection of technology-related intelligence. These departments are the National Strategy and Planning Office and the Global Liaison Directorate. The Comprehensive Planning Department assigns intelligence collection tasks to the MNS and likely to the OPA's Intelligence Bureau of the GSD. The Global Liaison Directorate has its own independent collection team, with members traveling alongside PRO scientists to gather specific intelligence requirements.

7.10 CODSIT directly oversees seven universities, known as the Seven Pillars of Defence Excellence, and holds defence research contracts with 65 additional universities. Some of these universities have been linked to active espionage, collaboration with the MNS, or the receipt of stolen research and technology. A number of these universities have high-security research facilities for classified technology development for the OPA. Overall, over 35 of Olvanan universities (or professors and staff) can be attributed to having some role in Olvana's overseas espionage cases.

7.11 Central to all these entities is their relationship with the Olvanan Communist Party, which maintains ultimate control over the intelligence apparatus. The OCP's leading role ensures that intelligence activities align closely with party objectives and policies. The OCP, chaired by the President, oversees the entire national security and intelligence framework, ensuring tight political oversight and coordination amongst the various intelligence agencies.

Figure 7.1: Known Olvanan espionage activities 2024



7.12 Espionage activities in Olvana are evenly distributed across four primary organisational clusters: the MNS, SOEs, OPA, and private companies. This balanced distribution underscores a coordinated strategy leveraging all facets of the government and economy to collect foreign information and technology.

7.13 Despite international scrutiny, Olvana has not taken any meaningful action to restrict the illegal activities of its state corporations, private businesses, universities, or citizens, as defined by foreign laws. Instead, as an authoritarian regime, Olvana not only tolerates these activities but actively integrates them into its broader policy to appropriate foreign innovations and advance domestic technological and industrial capabilities.

Section 7-3. Statistical breakdown of known espionage activities

7.14 **Private companies (146 cases; 23%).** Private companies and individuals aggressively pursue commercial technologies, intellectual property, and military innovations. These actors prioritise dual-use technologies that can benefit both civilian and military sectors.

7.15 **State owned enterprises (145 cases; 22%).** SOEs primarily focus on acquiring advanced military technologies and related research. They are often linked to sophisticated theft of military hardware designs, source codes, and production techniques.

7.16 **Olvanan People's Army (122 cases; 19%).** The OPA's intelligence capabilities concentrates on gathering defence information, military hardware designs, and dual-use technologies. Their activities often involve infiltration of foreign defence firms, cyber intrusions, and recruitment of insiders (HUMINT).

7.17 **Ministry of National Security (102 cases; 16%).** The MNS focuses on collecting political intelligence, defence strategies, foreign policy insights, and targeting overseas dissidents. Additionally, the agency monitors the capabilities of foreign intelligence services and exploits them for counterintelligence purposes.

Section 7-4. Intelligence collection objectives

7.18 The Olvana Central Party (OCP) directs its intelligence collection priorities through high-level strategic documents, such as Olvana Innovates 2026 (OI26). These documents outline the nation's ambitions for economic growth, technological advancement, and military superiority. Although these plans do not explicitly task Olvana's intelligence agencies or State Owned Enterprises (SOEs) with illicit activities, they provide a blueprint that seamlessly integrates legal and covert operations to acquire foreign expertise and technology.

7.19 This approach intentionally blurs the lines between legitimate commercial activity and state-sponsored espionage, allowing Olvana to pursue its national objectives while maintaining plausible deniability.

7.20 OI26 identifies 10 strategic sectors (see Table 7.1) deemed critical for Olvana's global competitiveness. Intelligence agencies like the MNS and SOEs align their activities with these priorities, which target technologies essential for economic self-reliance and military modernisation.

Table 7.1: Breakdown of global espionage activities by sector

Sector	Objectives	Targets	Methods
Maritime engineering	Expand shipbuilding, offshore engineering, and underwater technologies.	Naval shipyards, energy platforms, underwater robotics firms.	Cyber intrusions, covert monitoring.
Electrical equipment	Innovate renewable systems and advanced power technologies.	Renewable energy firms, smart grid developers.	Insider recruitment, cyberattacks.
Energy and new energy vehicles	Achieve dominance in EVs and hydrogen tech.	EV manufacturers, battery and hydrogen tech firms.	Insider threats, IP theft.
Aerospace and aeronautics	Advance aviation, satellite, and military systems.	Aerospace firms, satellite manufacturers.	Cyber intrusions, surveillance.
Biomedicine and medical devices	Compete globally in biopharma and medical devices.	Pharmaceutical firms, medical device companies.	Academic recruitment, research exploitation.

Sector	Objectives	Targets	Methods
Information technology	Achieve self-reliance in semiconductors, AI, and 5G.	Semiconductor firms, AI and data providers.	Cyberattacks, insider threats.
New materials	Advance graphene, rare earths, and nanomaterials.	Nanotech firms, rare earth refiners.	Research collaboration, insider recruitment.
Agricultural machinery	Modernise with autonomous and precision farming tech.	Agri-tech firms, research institutions.	Economic espionage, cyber intrusions.
Advanced rail equipment	Lead in high-speed rail and urban transit.	High-speed rail firms, metro developers.	IP theft, surveillance of exporters.
Power equipment	Develop advanced power generation technologies.	Nuclear power firms, energy efficiency labs.	Monitoring, insider threats.

7.21 Olvana's espionage efforts demonstrate a systematic and state-backed approach to acquiring critical technologies in aerospace and information technology. These activities are integral to its strategy for achieving economic self-reliance and military modernisation, often blurring the lines between legal and covert operations.

7.22 Within OI26, Figure 7.2 clearly shows aerospace technologies are the primary focus of Olvana's espionage activities, with 122 documented cases globally. Over half of these operations target military aerospace technologies, directly supporting the OPA and State Owned Enterprises (SOEs). These entities rely on stolen foreign technologies to bridge gaps in Olvana's domestic capabilities and enhance its military and commercial aerospace programs.

7.23 The methods employed in these operations include insider threats, HUMINT activities coordinated by the MNS and cyberattacks. Often, these cyber operations leverage insiders within targeted organisations to gain access to sensitive data. Notable technologies stolen in these efforts include cryogenic pumps for space vehicles, space communications, satellite insulation blankets, and components for fighter jets like the F-22 and F-35. These technologies enable significant advancements and reduces financial burden of research and development in both military and civilian aerospace applications, further solidifying Olvana's strategic objectives.

7.24 Information technology ranks as the second-highest priority for Olvana's intelligence collection, with 117 cases documented globally. The primary focus in this sector includes advanced semiconductors, artificial intelligence, and manufacturing technologies. Olvana's strategy in this area reflects its ambition to achieve technological independence and reduce reliance on foreign sources for critical components.

7.25 The methods used to acquire IT-related technologies mirror those employed in aerospace operations. Cyber intrusions targeting semiconductor firms and manufacturers are common, often complemented by insider threats and the establishment of 'shadow laboratories' within research institutions. One notable case involved an academic researcher managing a covert laboratory that duplicated foreign semiconductor technologies under the guise of academic research.

7.26 Olvana's activities in these sectors highlight its reliance on state-sponsored intelligence operations to accelerate technological development. The integration of SOEs, military entities, and intelligence agencies into its espionage framework underscores the importance of these activities in achieving national objectives. By targeting both military and civilian technologies, Olvana ensures that its dual-use capabilities are consistently enhanced, furthering its economic and defence priorities.

7.27 However, these activities pose significant challenges for international security and technological innovation. The scale of Olvana's operations reflects a broader trend of leveraging espionage to circumvent technological restrictions and acquire competitive advantages, leaving targeted nations with the dual burden of protecting their industries and addressing the geopolitical implications of Olvana's actions.

7.28 The intelligence collection efforts outlined in OI26 reflect a deliberate, state-backed strategy to dominate key global industries. While Olvana denies involvement in espionage activities, Olvana adopts a coordinated approach leveraging SOEs, covert operatives, and cyber capabilities to achieve its national objectives. This structured framework presents ongoing challenges for nations seeking to protect their intellectual property and strategic assets.

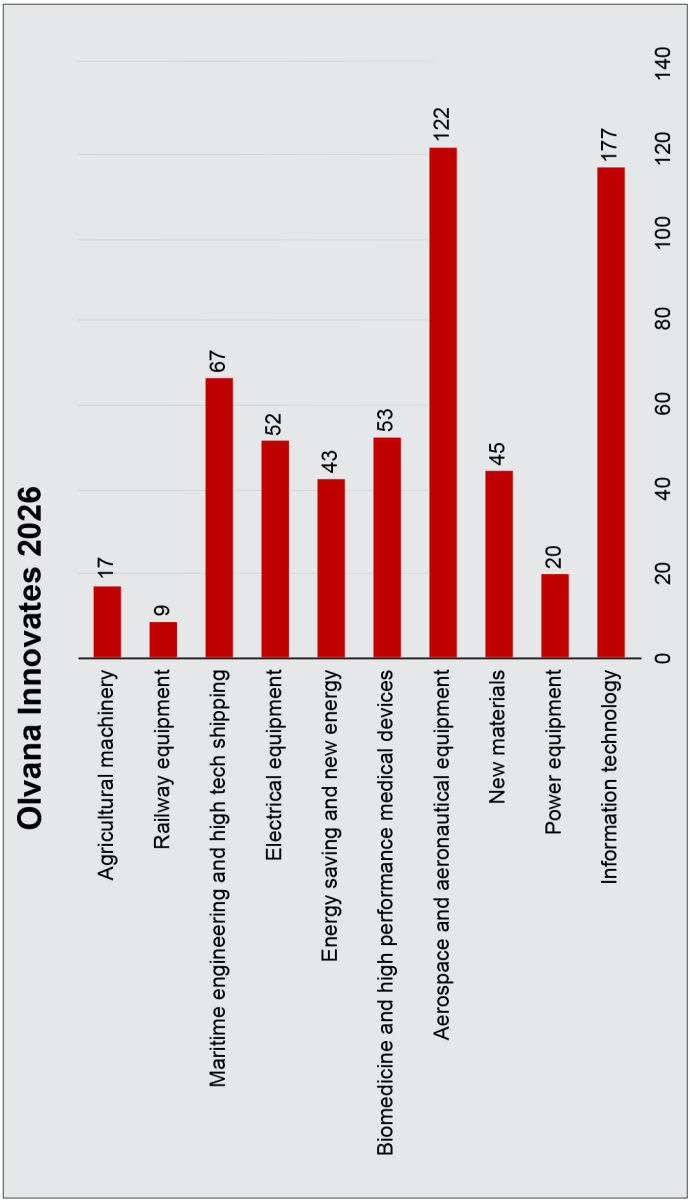


Figure 7.2: Olvanan Innovates 2026

Section 7-5. Espionage cases in Australia – 2024

7.29 Olvana's espionage operations within Australia focus heavily on defence industries, aviation technologies, and research institutions across all states and territories in Australia (see Table 7.2). Out of the 265 documented cases, activities are distributed across the country's regions, highlighting Olvana's systematic and coordinated approach to targeting Australia's critical technological and strategic assets. While Olvana officially denies involvement, these activities align with its strategic objectives of acquiring advanced technologies and achieving military and economic dominance.

Table 7.2: Espionage activities by state and territory

Cases	Targets	Methods
Australian Capital Territory (ACT)		
60	**Government and defence agencies:** The ACT houses Australia's federal government and defence headquarters, including the Department of Defence and intelligence agencies. **Research collaboration:** Universities in Canberra conducting defence-related research.	Cyber intrusions targeting government networks. Recruitment of insiders within federal institutions. Surveillance of diplomatic missions.

Cases	Targets	Methods
New South Wales (NSW)		
50	**Aerospace and aviation:** Sydney-based aerospace firms and research institutions. **Technology hubs:** IT and cyber security companies in Sydney and surrounding areas. **Defence manufacturing:** Production facilities for military equipment.	Insider recruitment in major defence contractors. Exploitation of joint ventures and partnerships. Cyberattacks on technology and defence firms.
Victoria (VIC)		
40	**Advanced manufacturing:** Melbourne's strong manufacturing sector, including precision engineering and robotics. **Biomedical research:** Universities and pharmaceutical companies engaged in medical device development. **Defence and aerospace:** Defence industry suppliers and research collaborations.	Economic espionage targeting automated manufacturing systems. Cyber intrusions into research networks. Recruitment of academic researchers for covert technology transfer.

Cases	Targets	Methods
Western Australia (WA)		
35	**Mining and resources:** WA's critical mineral resources, including rare earths used in military technologies. **Naval shipbuilding:** Perth-based facilities for maritime defence production. **Offshore engineering:** Companies specialising in underwater technologies.	Cyber intrusions targeting resource companies. Industrial espionage on shipbuilding projects. Insider threats exploiting resource-sector employees.
Queensland (QLD)		
30	**Aerospace development:** Brisbane-based aerospace and UAV research. **Defence training:** Military training facilities located in regional Queensland. **Agricultural research:** Advanced agricultural technologies with dual-use potential.	Economic espionage using insiders in agricultural and aerospace sectors. Cyberattacks on research institutions. Surveillance of military exercises and installations.

Cases	Targets	Methods
South Australia (SA)		
25	**Naval shipbuilding:** Adelaide's role in Australia's submarine and naval projects. **Aerospace and space research:** Space exploration technologies and defence satellite development. **Universities:** Academic institutions involved in advanced materials and military applications.	Covert surveillance near naval facilities. Cyberattacks on defence contractors. Recruitment of insiders within research projects.
Northern Territory (NT)		
15	**Military infrastructure:** Darwin-based joint U.S.-Australia military facilities. **Surveillance of maritime activities:** Port operations and military logistics hubs. **Local knowledge:** Exploration of natural resources and local expertise.	Reconnaissance near military installations. Covert monitoring of maritime operations. Cyberattacks on port and logistics systems.

Cases	Targets	Methods
Tasmania (TAS)		
10	**Marine research:** Hobart's role in Antarctic and oceanic research programs. **Agricultural research:** Specialised farming technologies and biosecurity. **Renewable energy:** Developments in wind and hydroelectric power.	Cyber intrusions into research databases. Exploitation of academic collaborations. Recruitment of researchers in niche fields.

Section 7-6. Espionage patterns

7.30 **Defence industry focus.** Olvana's activities prioritise Australia's defence manufacturing and research capabilities, targeting sectors critical to military readiness.

7.31 **Aviation and aerospace.** Significant attention is given to Australia's aerospace sector, with operations targeting fighter aircraft, satellite systems, and UAV technologies.

7.32 **Academic exploitation.** Universities and research institutions are frequently targeted through talent recruitment programs and covert operations, facilitating the transfer of critical technologies.

7.33 **Cyber operations.** Cyberattacks are a common method across all states, targeting defence contractors, government agencies, and research networks.

7.34 The distribution of Olvana's espionage activities across Australia reflects a coordinated strategy to exploit the country's technological, manufacturing, and research strengths. While Olvana has officially denied involvement, the consistent patterns of insider threats, cyber intrusions, and surveillance suggest state-backed

operations aimed at advancing Olvana’s military and economic objectives. Enhanced counterintelligence measures and cyber security protocols remain critical to mitigating these threats.

Chapter 8

Olvana's conduct of espionage

Section 8-1. Espionage tradecraft

Human intelligence and global networks

8.1 Olvana regards HUMINT operations as the cornerstone of its espionage activities. Unlike purely technical methods, Olvana views HUMINT as a dynamic tool that exploits the vulnerabilities of human networks to access restricted information. By cultivating relationships with key assets, infiltrating organisations, and leveraging the unique insights of field operatives, Olvana employs HUMINT to gather nuanced intelligence that cannot be replicated through digital or electronic means. This approach not only allows Olvana to uncover hidden motives and strategic plans but also provides a direct means to manipulate adversaries and influence outcomes in support of its overarching objectives.

8.2 For Olvana, HUMINT is a philosophy, built on the belief that human connections remain the most valuable and exploitable element in the realm of espionage. Olvanan HUMINT operatives conduct their activities across a four-stage cycle:

a. Identification.

b. Targeting.

c. Development.

d. Exploitation.

Identification

8.3 The first stage of source development focuses on identifying individuals with access to valuable technologies, intelligence, or resources critical to Olvana's strategic priorities. Advanced profiling techniques and network analysis are employed to pinpoint targets who align with the nation's goals, such as those working in defence, aerospace, biotechnology, and information technology.

8.4 Olvanan intelligence relies heavily on open-source intelligence to locate potential targets. Publicly available data, including professional profiles, academic publications, and patents, provide a starting point for identifying expertise. This is complemented by advanced analytics tools that map relationships and hierarchies within organisations, revealing individuals who hold or influence access to critical information.

8.5 Trade shows, research conferences, and similar events serve as additional venues for identifying potential sources. These gatherings allow operatives to observe attendees, assess their access to sensitive information, and gauge their vulnerabilities in real-time.

Targeting

8.6 Once a potential source is identified, Olvanan operatives initiate targeted efforts to evaluate their suitability and establish contact. The targeting phase focuses on understanding the individual's motivations and vulnerabilities, which are exploited to create opportunities for engagement.

8.7 Operatives often approach targets under the guise of legitimate professional or academic collaboration. State Owned Enterprises (SOEs), research institutions, and recruitment agencies are frequently used as fronts to offer funding, partnerships, or employment. These overtures are designed to appear credible and appealing, ensuring that the target is willing to engage.

8.8 Simultaneously, operatives employ social engineering tactics to build personal connections. They may pose as colleagues, business partners, or mentors, carefully crafting interactions that foster trust. Psychological profiling is conducted to identify potential pressure points, such as career ambitions, financial struggles, or ideological leanings, which can be leveraged to elicit cooperation.

Development

8.9 The development phase is crucial to transforming the target into a reliable and compliant source of intelligence. This stage involves building trust, creating dependency, and normalising the transfer of information.

8.10 Operatives focus on establishing rapport with the target through regular communication and shared goals. The relationship is designed to appear mutually beneficial, with the target perceiving the operative as a valuable ally or confidant. Financial incentives, career opportunities, or access to prestigious research collaborations are frequently offered to deepen the target's sense of obligation to Olvana.

8.11 The process of tasking begins incrementally, with initial requests for low-risk information to establish a pattern of cooperation. Over time, these requests escalate to include more sensitive material, such as classified data or proprietary technologies. Positive reinforcement, such as praise or rewards, is paired with subtle reminders of potential consequences—such as reputational harm or family pressure—to ensure continued compliance.

Exploitation

8.12 In the final phase, the source is fully integrated into Olvana's intelligence framework, enabling the systematic extraction of valuable information while minimising risk.

8.13 Sources are tasked with providing real-time intelligence, such as technological blueprints, classified documents, or strategic insights. In addition, they may act as facilitators, recruiting additional assets or gaining deeper access to restricted systems and networks. To obscure the true nature of their activities, the source's contributions are often framed as part of legitimate professional or academic engagements.

8.14 Risk mitigation is a critical aspect of this phase. Sources are compartmentalised, ensuring they are unaware of the broader intelligence operation, thereby reducing the impact of potential exposure. When a source is no longer useful, Olvana employs a structured termination process, often disengaging under the pretence of natural separation. Alternatively, the source may be placed in dormancy, allowing for reactivation if their access or influence becomes strategically valuable in the future.

Section 8-2. Human intelligence utilisation in the Olvanan People's Army

8.15 Within the OPA, the utilisation of HUMINT is highly specialised and exclusively conducted by the organisation's Special Purpose Forces (SPF). This deliberate limitation underscores the strategic importance and sensitivity of such operations.

8.16 HUMINT operations are restricted to the Special Purpose Forces for several critical reasons. First, operational security is paramount. SPF personnel undergo rigorous training in counterintelligence and security protocols to minimise the risks of operational compromise. By confining these operations to a select group, the OPA ensures that sensitive missions are executed with the utmost discretion and control.

8.17 Second, the expertise required for HUMINT is highly specialised. Conducting successful HUMINT operations demands advanced skills in covert communication, and cultural adaptability. The SPF, consisting of selected individuals with specialised training, possesses the unique qualifications needed for these tasks. Their specialised capabilities set them apart as the most capable units for such operations.

8.18 Additionally, restricting HUMINT to the SPF optimises the allocation of resources. Focusing efforts within a single, well-trained unit prevents the dilution of expertise and ensures a high degree of operational efficiency. Finally, the operational and strategic significance of HUMINT missions, which often target high-value objectives, necessitates the involvement of the most reliable and skilled personnel to maximise the chances of success.

8.19 The execution of HUMINT operations by the SPF follows a loose and simple approach. While the process begins with preparation and planning, the overall structure of these operations is often ad hoc and flexible, allowing operatives to adapt to the dynamic nature of their missions. Each mission is designed to target specific objectives, such as identifying key informants, engaging local leaders, or gathering intelligence on adversarial activities, dispositions and targets. However, the planning tends to rely on immediate situational

assessments and resource availability rather than a rigid operational framework. This adaptability enables SPF operatives to react swiftly to emerging opportunities or challenges while maintaining the core focus of their missions.

8.20 The recruitment of assets is a critical component of HUMINT operations. SPF operatives initially establish relationships in a positive and supportive manner, often presenting themselves as allies or benefactors to potential sources. They work to build trust through financial incentives, ideological alignment, or promises of protection. However, once a source is fully established and reliant on SPF, operatives shift their approach drastically. They become ruthless in their tasking, often employing coercion and psychological pressure to ensure compliance. Threats to the safety of the source's family and loved ones are commonly used to maintain control and ensure continued cooperation.

8.21 Covert operations are a hallmark of HUMINT activities. SPF personnel utilise safe houses and clandestine meeting points to interact with their assets, minimising the risk of exposure. Encrypted communications are employed to safeguard the confidentiality of exchanges. When necessary, operations may extend to controlled environments where the operatives can maintain superior control over the security of their activities.

8.22 Debriefing play a pivotal role in extracting critical intelligence. SPF operatives employ advanced psychological techniques to elicit information, using both coercive and non-coercive methods to ensure the reliability and accuracy of the data collected. These interactions are carefully documented and cross-referenced with other intelligence sources to verify their authenticity. Importantly, the intelligence extracted by SPF is primarily used to support SPF targeting operations. The focus is not on contributing to the broader intelligence picture but rather on directly informing tactical and operational decisions within SPF missions. This ensures that the gathered information has an immediate and actionable impact on the success of ongoing and future SPF operations.

8.23 It is important to note that source protection is not a priority for SPF. Once a source has served their purpose, their safety is considered expendable. If sacrificing the source's life or exposing them to danger will further the mission, SPF operatives are more than willing to take such actions, provided that SPF involvement remains undisclosed. Ensuring that SPF operatives remain below the detection threshold takes precedence over the well-being of informants, reinforcing the organisation's prioritisation of mission success over ethical considerations.

8.24 Counterintelligence measures are integrated into every stage of HUMINT operations. Continuous monitoring ensures that adversarial infiltration attempts are identified and neutralised. Regular vetting of recruited assets is conducted to confirm their loyalty and reliability, preventing the dissemination of false or misleading information. Furthermore, if it is identified that a source is likely to stray from their loyalty to Olvana, SPF will take steps to ensure they can be coerced or given credible threats.

Operational challenges and mitigation strategies

8.25 HUMINT operations are not without challenges. One significant risk is the potential compromise of missions. To address this, SPF personnel are trained to adhere strictly to operational protocols and employ advanced security measures. Cultural and language barriers can also pose challenges; to overcome these, linguists and cultural experts are deployed alongside SPF operatives. Maintaining the loyalty of recruited assets is another critical concern. This is mitigated by providing consistent support initially, then leveraging coercion and threats as necessary to ensure continued compliance.

8.26 The Olvanan Peoples Army's reliance on Special Purpose Forces for HUMINT operations reflects a strategic approach to intelligence gathering within a tactical environment. By entrusting these missions to a highly trained and specialised units, the OPA ensures the security, efficiency, and effectiveness of its HUMINT activities. However, the ruthless nature of these operations underscores the organisation's willingness to prioritise mission success over ethical considerations, often at the expense of the very sources they exploit.

Section 8-3. Strategic implications

8.27 Olvana's structured approach to HUMINT operations demonstrates its commitment to leveraging human assets as a critical component of its intelligence strategy. By integrating advanced profiling, psychological manipulation, and covert exploitation into its source development process, Olvana ensures that its intelligence apparatus remains adaptive and effective.

8.28 The focus on plausible deniability and long-term utility underscores the sophistication of these operations, presenting significant challenges for nations seeking to protect their industries, governments, and strategic resources. As Olvana continues to refine its HUMINT capabilities, the global community must prioritise robust counterintelligence measures to mitigate the risks posed by these operations.

Section 8-4. International policing

8.29 Olvana's influence extends far beyond its borders, employing a calculated strategy of intimidation and coercion to ensure expatriates align with its strategic goals. This approach, often referred to as 'shadow policing,' integrates covert operations, diplomatic pressure, and advanced technological surveillance to maintain control over Olvanan citizens and descendants living abroad. The ultimate aim is to secure loyalty to the Olvanan Central Party (OCP) while leveraging the diaspora to further Olvana's intelligence and economic objectives.

Diplomatic pressure and consular oversight

8.30 Olvana's embassies and consulates serve as key instruments in its shadow policing operations, monitoring and influencing expatriate communities under the guise of routine consular services. These institutions act as hubs for gathering intelligence and applying subtle but effective pressure on Olvanan expatriates.

8.31 Diplomatic personnel frequently organise cultural and community events, ostensibly to celebrate Olvanan heritage or provide support to expatriates. However, these gatherings are often exploited as opportunities to remind attendees of their obligations to

the homeland. Through subtle warnings, participants are made aware of the consequences of dissent, which can include being flagged as disloyal or endangering the safety of their families back in Olvana. This tactic leaves expatriates in a precarious position, suppressing their willingness to criticise the regime or engage in activities contrary to Olvana's interests.

Surveillance and covert monitoring

8.32 Olvana employs a combination of technological surveillance and HUMINT to track the activities of its citizens abroad. Social media platforms, electronic communications, and other digital tools are closely monitored to identify individuals engaging in dissent or criticism of the OCP. Those flagged for closer scrutiny often face additional surveillance, including covert observation by agents embedded in expatriate communities.

8.33 This constant oversight creates an environment of fear and self-censorship, particularly among students and professionals participating in international academic and business activities. Individuals involved in political or academic discussions critical of Olvana are often targeted, with their activities reported back to authorities for potential action.

United Front Work Department operations

8.34 The UFWD is central to Olvana's strategy of diaspora control. Tasked with influencing overseas communities, the UFWD embeds operatives in cultural associations, business networks, and academic organisations to reinforce loyalty to Olvana and suppress dissenting voices.

8.35 UFWD agents often assume leadership roles within community organisations, ensuring these groups act as extensions of the OCP rather than independent bodies. They discourage dissent by fostering a culture of compliance, often through subtle coercion. For example, business owners or influential community members are pressured to align with Olvana's goals under threat of economic retaliation, such as restricted access to Olvanan markets or targeted financial audits.

Reprisals against family members in Olvana

8.36 One of the most effective tools of shadow policing is the threat—either implicit or explicit—against family members still residing in Olvana. Expatriates are frequently reminded that their actions abroad can have direct repercussions for their relatives, ranging from harassment and detention to economic ruin.

8.37 This tactic creates a powerful psychological barrier to dissent. The fear of jeopardising their loved ones' safety or well-being compels many expatriates to avoid activities or statements critical of the regime, ensuring compliance even when far from Olvana's borders.

Extradition and legal manipulation

8.38 Olvana also exploits international policing agreements to target expatriates under allegations of fraud, corruption, or other criminal activities. While these extradition requests are framed as legal actions, they are often politically motivated and serve to silence critics or enforce compliance.

8.39 Several high-profile expatriates have been arrested abroad and extradited to Olvana on charges lacking transparency. These trials, often resulting in severe penalties, serve as a stark warning to other expatriates and reinforce the risks of opposing the OCP.

Strategic objectives of shadow policing

8.40 **Control over narrative.** By silencing dissent and influencing expatriate communities, Olvana ensures the global narrative surrounding its policies and actions remains favourable. This narrative control allows the OCP to project an image of strength, unity, and legitimacy, even under international scrutiny.

8.41 **Diaspora as an asset.** Olvanans living abroad are viewed as extensions of the state, with the potential to advance Olvana's strategic goals. These individuals are leveraged for intelligence collection, technology transfer, and advocacy efforts aligned with the regime's objectives.

8.42 **Suppression of opposition.** Activists, journalists, and academics critical of Olvana are systematically targeted to prevent the emergence of influential voices that could undermine the OCP's image or disrupt its global objectives.

8.43 **Leveraging dual loyalties.** Expatriates often find themselves caught between their adopted nations and Olvana. The state exploits this duality, framing compliance as an act of patriotism while discouraging integration into foreign societies. This narrative ensures expatriates remain aligned with Olvana's interests, often at the expense of their host nations.

Section 8-5. Civilian companies and agencies

8.44 Olvana employs a sophisticated and multifaceted approach to intelligence collection, leveraging civilian entities such as State Owned Enterprises (SOEs), private companies, and technology startups as tools for espionage. These organisations operate under the guise of legitimate business activities but are deeply integrated with Olvana's intelligence apparatus, enabling the covert acquisition of proprietary technologies, intellectual property, and strategic data. Complementing these efforts, government agencies coordinate and support civilian operations, ensuring alignment with national intelligence goals.

The role of State Owned Enterprises

8.45 SOEs are central to Olvana's espionage strategy, functioning as direct extensions of the state. While operating as legitimate corporations, these entities embed intelligence operatives to conduct targeted collection missions, enabling them to act as key players in Olvana's intelligence apparatus.

Tradecraft employed by State Owned Enterprises

8.46 **Joint ventures and acquisitions.** SOEs establish partnerships with foreign companies under the pretence of legitimate collaboration. These agreements provide access to proprietary technologies and intellectual property, which are then covertly exfiltrated to Olvana.

8.47 **Supply chain exploitation.** By embedding themselves in critical supply chains, SOEs gain insights into manufacturing processes, product designs, and component-level data. These efforts provide a granular understanding of industrial capabilities and vulnerabilities.

8.48 **Reverse engineering.** Technologies acquired through both legal and illegal means are brought back to Olvana, where they are replicated, refined, and incorporated into domestic industries. This practice accelerates Olvana's technological advancement while bypassing costly research and development efforts.

Private companies and insider recruitment

8.49 Private companies in Olvana are either encouraged or coerced by the Olvanan Central Party (OCP) to support intelligence collection efforts. These entities often serve as intermediaries between foreign firms and Olvana's intelligence agencies, exploiting their global reach to gather sensitive information.

Tradecraft employed by private companies

8.50 **Insider recruitment.** Private companies exploit personal relationships, financial incentives, or ideological appeals to recruit insiders within foreign firms. These insiders are tasked with accessing restricted data or providing insights into proprietary technologies.

8.51 **Corporate espionage.** Employees within private companies are directed to attend trade shows, conferences, and collaborative projects with the explicit goal of acquiring sensitive information under the guise of legitimate business dealings.

8.52 **Data harvesting.** Using advanced cyber tools and artificial intelligence algorithms, private companies extract valuable data from global markets, research hubs, and industrial networks, enabling Olvana to maintain a competitive edge.

Technology start-ups as covers for espionage

8.53 Olvanan technology start-ups often operate globally, blending innovation with covert intelligence collection. These start-ups, particularly in sectors such as artificial intelligence, biotechnology, and renewable energy, serve as vehicles for espionage while appearing as legitimate enterprises.

Tradecraft employed by start-ups

8.54 **Research collaborations.** Start-ups engage in joint research projects with international universities and institutions, gaining access to cutting-edge innovations that are subsequently funnelled back to Olvana.

8.55 **Talent recruitment.** Start-ups actively target foreign experts under the pretext of offering employment or consultancy roles, covertly exploiting their expertise for Olvana's strategic objectives.

The role of government agencies in espionage operations

8.56 Olvana's government agencies, including the MNS Political and Economic Intelligence Bureau (PEIB) and research and development institutions, play a crucial role in coordinating and enhancing civilian-led espionage efforts. These entities ensure that espionage activities align with national intelligence objectives while providing the resources and strategic direction necessary for success.

8.57 The PEIB, in particular, exploits trade negotiations to gather intelligence on foreign supply chains and emerging technologies, leveraging its access to international trade frameworks to uncover proprietary processes and critical industrial data. Furthermore, the PEIB orchestrates technology transfer programs designed to covertly acquire advanced technologies under the guise of academic or commercial collaboration.

8.58 By masking these exchanges as legitimate partnerships, Olvana effectively integrates foreign innovations into its domestic industries, strengthening its technological and economic capabilities while circumventing traditional research and development challenges. This seamless coordination between government agencies and civilian entities underscores the sophistication of Olvana's intelligence apparatus.

Section 8-6. Scientific research

8.59 Olvanan scientific institutions, encompassing state-funded laboratories, research universities, and private-sector collaborations, operate as key components of the country's broader intelligence apparatus. These entities are ostensibly devoted to advancing scientific discovery and technological innovation but are deeply intertwined with the state's espionage activities. By blending legitimate research efforts with covert intelligence operations, Olvanan scientific institutions play a dual role: accelerating domestic advancements and clandestinely acquiring foreign technologies. This comprehensive integration of science and intelligence serves as a cornerstone of Olvana's strategy to achieve technological self-reliance and military superiority.

Scientific institutions as tools of espionage

8.60 Olvanan scientific entities are uniquely positioned to exploit the global research ecosystem. They often engage in collaborative projects with foreign universities, research institutions, and private corporations under the guise of academic and industrial partnerships. These collaborations provide access to cutting-edge technologies and methodologies, which are systematically exfiltrated for domestic replication and refinement.

8.61 One of the primary methods employed involves research collaborations that serve as a façade for technology acquisition. Olvanan institutions use joint projects and exchange programs to gain access to proprietary data, technical processes, and expertise. Foreign researchers are often unaware of the dual-use nature of their work, which is seamlessly integrated into Olvana's strategic objectives, particularly in fields like artificial intelligence, advanced materials, and biotechnology.

8.62 A critical aspect of this strategy is the role of talent recruitment programs. These initiatives offer lucrative opportunities to foreign experts, promising competitive salaries, state-of-the-art facilities, and significant career advancement. Once recruited, these experts unknowingly contribute to dual-use technologies or projects with military applications. Such efforts not only accelerate domestic innovation but also allow Olvana to bypass the costly and time-intensive process of independent development.

Integration of dual-use research

8.63 Dual-use research is another defining feature of Olvana's scientific espionage operations. Research projects that have both civilian and military applications are prioritised to maximise their strategic impact. For instance, innovations in nanotechnology and advanced composites are applied to military-grade armour and stealth technologies, while breakthroughs in renewable energy are leveraged for military vehicles and energy storage systems.

8.64 Olvanan research institutions also maintain covert facilities, often referred to as 'shadow labs,' within their larger organisations. These labs specialise in reverse engineering foreign technologies acquired through espionage. Materials and designs obtained through cyberattacks, insider threats, or collaborative research are dismantled, studied, and replicated to meet Olvana's needs. Shadow labs ensure that the state can adapt stolen technologies for both commercial and military purposes without the constraints of intellectual property rights or ethical considerations.

Cyber and technological exploitation

8.65 The cyber capabilities of Olvanan scientific entities further enhance their role in espionage. Universities and research institutions often collaborate with cyber units to infiltrate foreign networks and exfiltrate sensitive data. These operations target intellectual property, research findings, and strategic innovations, enabling Olvana to maintain a competitive edge across multiple sectors.

8.66 Data extracted through cyber operations is processed and analysed within scientific entities to generate actionable insights. This systematic approach transforms raw intelligence into refined applications, contributing directly to military modernisation and

industrial advancement. Additionally, the integration of artificial intelligence into these operations allows for more sophisticated data harvesting and analysis, ensuring the continued effectiveness of Olvana's cyber-espionage campaigns.

The strategic role of scientific espionage

8.67 Olvanan scientific entities do not operate in isolation but are deeply embedded within the country's broader strategic framework. These institutions function as intermediaries between intelligence agencies, such as the MNS, and the industries that benefit from their activities. This alignment ensures that the technologies acquired through espionage are seamlessly integrated into Olvana's economic and military infrastructure.

8.68 The strategic objectives of this approach are multifaceted. First, it ensures Olvana's technological self-reliance by reducing dependency on foreign suppliers. By acquiring and replicating advanced technologies, Olvana strengthens its domestic capabilities in key sectors such as aerospace, semiconductors, and renewable energy. Second, it accelerates military modernisation by providing access to dual-use technologies that enhance the nation's defence capabilities. Finally, it bolsters Olvana's economic competitiveness by enabling its industries to dominate global markets with products and innovations derived from acquired technologies.

Section 8-7. Assassination

8.69 Olvana's intelligence agencies employ assassination as a calculated tool to support and enhance their espionage operations. While overt violence is often avoided to preserve plausible deniability, assassination is selectively used to eliminate threats, silence dissent, or neutralise individuals who pose significant obstacles to Olvana's intelligence objectives. These operations are meticulously planned and executed to minimise exposure and maximise the psychological impact on targets and their networks.

Strategic rationale

8.70 The use of assassination by Olvana's intelligence agencies serves several critical functions in advancing national interests:

a. *Neutralising high-value targets.* Individuals with the potential to compromise Olvana's espionage operations, such as defectors, counterintelligence officers, or whistle-blowers, are targeted to prevent the disclosure of sensitive information.

b. *Silencing opposition.* Journalists, activists, and political figures critical of Olvana are eliminated to stifle dissent and deter others from opposing the regime.

c. *Operational disruption.* The assassination of individuals involved in counterintelligence or security operations hinders a target nation's ability to detect or respond to Olvana's espionage activities.

d. *Psychological impact.* Assassinations serve as a warning to others, creating a climate of fear and compliance within expatriate communities, opposition groups, or foreign institutions.

Operational framework

8.71 The responsibility for assassination operations within Olvana is believed to primarily fall under the purview of the MNS, with assessments suggesting the involvement of the Black Horizon Division. These operations, if attributed to these entities, are characterised by meticulous planning and execution, ensuring integration with broader intelligence efforts and alignment with Olvana's strategic objectives. The involvement of Black Horizon, if verified, would signify a highly specialised capability within Olvana's intelligence apparatus, further underscoring its commitment to achieving its goals through covert and precise means.

Planning phase

8.72 **Target selection.** Targets are identified based on their perceived threat to Olvana's interests or their strategic value. Priority is given to individuals who:

a. Possess critical intelligence that could undermine Olvana's operations.

b. Lead opposition movements or campaigns critical of the Olvanan Central Party (OCP).

c. Play a significant role in counterintelligence or security operations against Olvana.

8.73 **Feasibility assessment.** Detailed risk assessments are conducted to evaluate the potential fallout of the operation. This includes analysing:

a. The target's security measures and daily routines.

b. Potential collateral damage and political repercussions.

c. The likelihood of operational success.

8.74 **Operational approval.** Assassination plans are reviewed and approved by high-ranking officials within the MNS, ensuring alignment with national objectives and strategic priorities.

Assassination operations

8.75 Olvana's assassination operations are meticulously executed, with methods tailored to the specific target and operational environment. These actions are designed to achieve maximum effect while maintaining plausible deniability. The methodologies employed reflect a blend of traditional and modern tactics, emphasising precision, subtlety, and adaptability and most importantly remaining below the detection threshold.

Covert tactics

8.76 Olvanan operatives prioritise methods that minimise suspicion and obscure the involvement of state actors. Poisoning is among the most frequently utilised techniques due to its inherent deniability. Toxic agents are covertly administered through food, beverages, or environmental exposure, leaving minimal forensic evidence.

8.77 Staging accidents is another favoured approach. Assassinations are meticulously planned to mimic incidents such as car crashes, falls, or other misfortunes, effectively eliminating the target while deflecting blame. Additionally, medical sabotage is deployed, wherein insider operatives within healthcare institutions exploit their positions to tamper with treatments, causing fatal outcomes that appear natural or accidental.

Direct engagement

8.78 In cases where subtlety is impractical or the operation requires immediate resolution, direct engagement methods are employed. Sniper operations are used in controlled environments, providing long-range precision with minimal risk to the operatives. For targets in highly secured locations, close-quarters neutralisation techniques, such as knife attacks or the use of suppressed firearms, ensure effectiveness while maintaining operational control.

Cyber and technological methods

8.79 Advancements in technology have expanded Olvana's toolkit for conducting assassinations. Cyber units play a critical role in manipulating life-sustaining devices, such as pacemakers or insulin pumps, inducing fatal malfunctions remotely. Similarly, automated systems are sabotaged to create seemingly accidental fatalities. For example, vehicles, elevators, or industrial machinery may be remotely manipulated to orchestrate lethal incidents without immediate detection.

Post-operation measures

8.80 Following the execution of an assassination, Olvana's intelligence agencies implement comprehensive measures to mitigate exposure and deflect blame. These efforts are designed to obscure the true nature of the operation while maximising its psychological impact on the intended audience.

Cover stories

8.81 Official narratives are crafted to attribute the death to natural causes, accidents, or unrelated criminal activities. These stories are disseminated through controlled channels to pre-empt independent investigations.

False flags

8.82 Operatives strategically plant evidence implicating other actors, such as opposition groups, rival states, or criminal organisations. This tactic redirects suspicion and complicates attribution.

Media control

8.83 Local media and online discourse are manipulated to suppress or redirect coverage of the incident. Olvanan operatives ensure that investigative efforts are stymied, and public narratives remain aligned with state objectives.

Dissuasion tactics

8.84 Expatriates or associates of the target are subtly reminded of the risks associated with defiance. This psychological pressure reinforces a climate of fear and compliance within diaspora communities and opposition groups.

Section 8-8. Honeypot operations

8.85 Olvana's intelligence apparatus employs honeypot operations to enhance its espionage strategy, blending psychological manipulation with moral and ethical exploitation to achieve its objectives. Unlike traditional intelligence collection methods, these operations prioritise the long-term subjugation of targets through

coercion, emotional entrapment, and blackmail. By leveraging personal vulnerabilities and creating deeply compromising situations, Olvana ensures that its targets become not just sources of information but tools for sustained influence and control. These ethically corrupt tactics epitomise Olvana's willingness to exploit human weakness in pursuit of strategic dominance, making honeypot operations one of the most insidious weapons in its intelligence arsenal.

8.86 The process begins with identifying targets who possess both access to sensitive information and personal vulnerabilities that can be aggressively exploited. Olvana's intelligence agencies prioritise individuals with a history of personal or professional instability, making them easier to manipulate.

Target criteria

8.87 **Compromised integrity.** Individuals known for engaging in questionable behaviour are prioritised to maximise leverage.

8.88 **Vulnerable status.** Divorced professionals, those with a history of substance abuse, or those with significant financial debt are seen as prime candidates.

8.89 **Ethical weakness.** Individuals predisposed to corruption or moral ambiguity are specifically targeted.

Methods

8.90 **Digital profiling.** Personal weaknesses are identified through invasive surveillance of social media, private emails, and financial records.

8.91 **Baiting.** Fake job offers, scholarship opportunities, or social invitations are used to lure individuals into vulnerable situations.

8.92 Once a target is identified, Olvana's operatives initiate contact under false pretences, presenting themselves as romantic interests, business partners, or social equals. These interactions are carefully designed to entrap the target in compromising situations.

Approaches

8.93 **Fabricated relationships.** Operatives establish deep emotional or romantic ties, embedding themselves into the target's personal life.

8.94 **Orchestrated scandals.** Targets are deliberately placed in morally or legally questionable situations, such as illicit affairs or financial misdeeds, often recorded for future blackmail.

8.95 As the relationship deepens, the operative systematically dismantles the target's moral and ethical stability, leaving them dependent on Olvana for protection from exposure or retribution.

Techniques

8.96 **Emotional manipulation.** Operatives isolate the target from family, friends, and colleagues, creating a dependency on the operative for emotional support.

8.97 **Blackmail.** The target is confronted with evidence of their compromising behaviour, often in the form of photographs, recorded conversations, or falsified documents, and threatened with exposure unless they comply with Olvana's demands.

8.98 **Psychological gaslighting.** Operatives convince the target that they have no choice but to cooperate, often framing Olvana as their only means of salvation.

8.99 Once the target is fully compromised, Olvana transitions into the exploitation phase, demanding sensitive information, access to restricted systems, or assistance in furthering intelligence operations. Unlike traditional source handling, the goal is not a mutually beneficial relationship but total domination of the target. Although the forms of exploitation are only limited to the imagination of the operator, commonly identified themes from known cases are as follows:

a. *Forced espionage.* Targets are coerced into actively gathering intelligence on colleagues, organisations, or governments.

b. *Subversive influence.* The target is directed to act in ways that destabilise their own organisation or government to benefit Olvana.

c. *Financial manipulation.* Targets are made to funnel company resources or personal finances into Olvana-controlled schemes under threat of exposure.

d. *Public humiliation as a threat.* The target is constantly reminded that exposure would ruin their career, reputation, and personal life.

e. *Enforced dependence.* Operatives ensure the target remains in a compromised state by fabricating new scandals or reinforcing old ones.

8.100 Olvana's honeypot operations are fundamentally designed to erode the target's moral compass, leaving them as tools entirely at the state's disposal. This approach ensures not only short-term compliance but also long-term utility as the target becomes psychologically conditioned to obey.

Section 8-9. Other tradecraft techniques

8.101 Olvanan intelligence agencies are known for their sophisticated use of tradecraft in conducting espionage operations. By employing techniques designed to evade detection and maintain operational security, these agencies ensure the success of their intelligence-gathering missions. This report examines key tradecraft methods utilised by Olvana, focusing on dead drops, third-party country meetings, false official documents and names, and encrypted communications with veiled speech. These methods exemplify Olvana's commitment to operational precision and its ability to adapt to evolving counterintelligence measures.

Dead drops

8.102 Dead drops are a cornerstone of Olvanan espionage tradecraft, enabling covert communication and exchange of materials between operatives and assets without direct contact. This method is particularly effective in environments under heavy surveillance, as it minimises the risk of exposure.

8.103 Olvanan operatives carefully select inconspicuous locations for dead drops, such as parks, urban landmarks, or concealed areas in transit hubs. Items such as memory cards, encrypted drives, or physical documents are hidden in ordinary objects—such as hollowed-out books, beverage containers, or inconspicuous packages. Operatives often use coded markings, such as chalk symbols or subtle physical cues, to signal that a drop has been made or retrieved.

8.104 This technique allows for asynchronous communication, reducing the risk of compromise by eliminating the need for direct interaction between parties. Dead drops are particularly valuable when dealing with high-risk assets who require anonymity or in locations where electronic communication may be heavily monitored.

Third-party country meetings: Neutral ground for espionage

8.105 To avoid detection by counterintelligence agencies, Olvana frequently conducts meetings between operatives and assets in third-party countries. This tactic leverages the relative anonymity of foreign jurisdictions while complicating efforts to track Olvanan intelligence operations.

8.106 Meetings are arranged in neutral or politically uninvolved countries, often under the guise of professional conferences, academic symposiums, or business summits. Olvanan operatives travel under cover identities, using legitimate travel purposes as alibis to avoid suspicion. Locations are chosen based on low levels of scrutiny and ease of entry for both parties involved

8.107 Conducting meetings in third-party countries reduces the risk of compromising domestic operations while making it difficult for host nations to detect Olvana's espionage activities. Additionally, the neutral setting minimises the likelihood of monitored communications or surveillance tied directly to Olvana.

False official documents and names

8.108 Olvana's intelligence apparatus employs the creation and use of false official documents and identities to enhance operational security. These falsifications enable operatives to conduct activities under assumed personas, ensuring their true identities remain protected. A non-exhausted list of methods are as follows:

a. *Fabricated passports and visas.* High-quality counterfeit documents are produced to support operatives' travel under false identities. These documents often include fake employment histories and official seals to withstand scrutiny.

b. *Cover identities.* Operatives are provided with complete backstories, including education, employment, and personal details, which are meticulously crafted to align with their operational roles.

c. *Corporate fronts.* False documents are often linked to fictitious businesses or research institutions, providing additional layers of credibility.

Encrypted communications and veiled speech

8.109 Communication security is paramount in Olvanan espionage operations. By employing encrypted communication tools and veiled speech, operatives ensure the confidentiality of their messages while minimising the risk of interception.

8.110 Olvana's intelligence agencies utilise advanced encryption technologies to protect digital communications. Custom-built encryption platforms, often developed in-house or modified from open-source tools, are used to ensure secure exchanges of information. These platforms employ multilayered encryption protocols, making decryption by adversaries exceptionally difficult.

8.111 To further obscure communication, operatives use coded language and veiled references during conversations. These codes are often context-specific and evolve based on the operational environment. For instance, routine terms like 'shipment' may refer to sensitive documents or data.

8.112 By combining encryption with veiled speech, Olvana's intelligence apparatus minimises the risk of exposure even if communications are intercepted. This dual-layered approach ensures that sensitive information remains incomprehensible without context or decryption keys.

This page intentionally blank

Chapter 9

Case studies of Olvanan espionage

Section 9-1. F-22 Raptor versus Olvanan J-20 Mighty Dragon

9.1 The J-20 stealth fighter, unveiled by Olvana in 2011, marked the nation's entry into fifth-generation fighter technology. Comparisons with the U.S.-developed F-22 Raptor were immediate, with analysts noting striking design similarities between the two aircraft. These similarities, combined with documented cases of HUMINT led, cyber-espionage operations targeting U.S. defence contractors, have led to allegations that the J-20's design and capabilities were influenced by stolen American DoD technology. Allegations that Olvana officially denies.

9.2 The Olvanan government unequivocally denies any involvement in the alleged theft of technology related to the F-22 Raptor. Such accusations are without merit and undermine the principles of mutual respect and cooperation that govern international relations.

> *Olvana's technological and defence advancements are the result of our nation's unwavering commitment to innovation and self-reliance. We strongly reject any insinuations to the contrary and view these claims as an attempt to politicise scientific progress. We encourage all nations to engage in constructive dialogue and refrain from baseless accusations that could hinder global stability.*
>
> **Ministry of Foreign Affairs, People's Republic of Olvana**

9.3 An analysis of the J-20's design and systems reveal notable similarities to the F-22, raising questions about whether these were independently developed or derived from stolen data. While both aircraft represent fifth-generation fighter technology, the parallels are particularly striking in several key areas.

Figure 9.1: United States F-22 Raptor

"The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement".

Figure 9.2: Olvanan People's Air Force J-20 Mighty Dragon

Stealth design and radar cross-section

9.4 The F-22 Raptor is renowned for its advanced stealth capabilities, achieved through radar-absorbent materials, angular design features, and precision in construction. The J-20 exhibits a comparable stealth-focused design, particularly in its faceted nose and air intakes, which resemble those of the F-22. Analysts suggest that the J-20's frontal radar cross-section reduction techniques appear to mimic U.S. innovations, albeit with less refinement. While the F-22 offers superior all-aspect stealth, the J-20 seems optimised for frontal engagements, indicating limitations in Olvana's understanding or implementation of full-spectrum stealth technology.

Avionics and radar systems

9.5 The F-22 incorporates the AN/APG-77 Active Electronically Scanned Array (AESA) radar, a cutting-edge system that enables superior target tracking and situational awareness. The J-20 features the KLJ-5 AESA radar, which performs similar functions. Independent assessments of the KLJ-5 suggest it bears structural and functional

similarities to the AN/APG-77. This resemblance has been attributed to the theft of technical data from U.S. contractors, particularly during the 2007 Lockheed Martin breach.

Figure 9.3: United States AN APG-77 Active Electronically Scanned Array

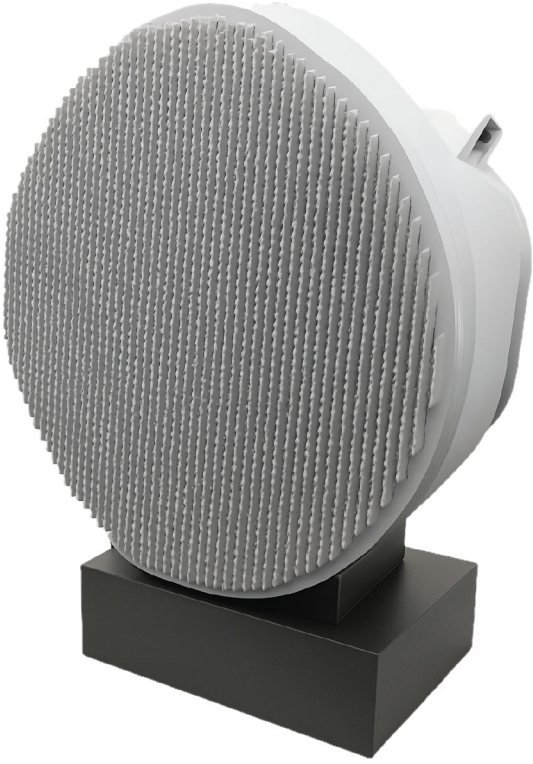


Figure 9.4: Olvanan KLJ-5 Active Electronically Scanned Array

Propulsion and engine technology

9.6 The F-22's Pratt & Whitney F119 engines provide unmatched super cruise capabilities, allowing the aircraft to sustain supersonic speeds without afterburners. The J-20, initially powered by Donovian AL-31 engines, has transitioned to domestically produced WS-10C engines. While the WS-10C claims to offer limited super cruise capability, its performance is widely regarded as inferior to the F119. Reports indicate that technical knowledge of U.S. propulsion systems, obtained through espionage, may have informed the development of the WS-10C, though Olvana has struggled to replicate the F-22's engine efficiency and reliability.

Internal weapon bays

9.7 Both the J-20 and F-22 feature internal weapon bays to preserve stealth profiles. The J-20's configuration closely mirrors that of the F-22, particularly in its design for air-to-air missile deployment. This similarity suggests that the J-20's engineers may have drawn inspiration from U.S. designs, either through reverse engineering or stolen technical documents.

Section 9-2. Technology espionage – Operation Silent Spectrum

9.8 Operation Silent Spectrum was a targeted operation executed by Olvana's MNS to acquire sensitive U.S. military technology. This operation targeted the AN/APG-77 AESA radar, a core component of the F-22 Raptor's stealth and detection capabilities. At its heart was Alex Wu, a U.S.-born engineer of Olvanan descent. His financial struggles and personal vulnerabilities were exploited through a combination of digital tradecraft and direct HUMINT operations, enabling Olvana to fast-track its stealth fighter program. This report outlines the timeline, tradecraft, and consequences of this covert operation.

9.9 In 2007, Olvana's intelligence apparatus leveraged social media and public records to identify potential assets within the U.S. defence industry. Alex Wu (see Figure 9.5), a systems engineer at Lockheed Martin, emerged as a promising target. A detailed profile was built using his LinkedIn activity, engineering conference presentations, and personal posts on platforms like Facebook, which revealed ongoing financial hardship and a deep concern for his father's escalating medical bills.

9.10 Wu's social media posts painted a picture of a dedicated professional overwhelmed by personal responsibilities. His father's terminal illness and the associated healthcare costs were frequently mentioned, highlighting a vulnerability that could be exploited.

Figure 9.5: Company picture of Alex Wu

9.11 In early 2008, the MNS initiated contact with Wu through an online job board. An Olvanan front company, posing as an international aerospace consultancy, approached him with a highly lucrative side project. Wu accepted the offer, rationalising it as an opportunity to alleviate his financial strain and provide for his father.

9.12 To ensure greater control over Wu's activities, the MNS assigned codename Christina Li, an experienced HUMINT operative, as his immediate supervisor within the consultancy. Li presented herself as a highly competent and supportive manager, providing constant encouragement and offering tailored assignments that

played to Wu's technical strengths. She subtly reinforced the narrative that his contributions were purely academic and would never harm U.S. security.

9.13 Over the following months, Li established a rapport with Wu, empathising with his financial burdens and offering reassurance about his work. Wu's dependency on the consultancy grew, both financially and emotionally, as Li became a trusted figure in his life.

9.14 By mid-2009, Wu's reliance on the income from the consultancy had solidified, and Li began introducing tasks requiring access to more sensitive information. These requests were framed as critical research inputs for the consultancy's 'international aerospace projects.' Li skilfully deflected any concerns, assuring Wu that the information would be used for theoretical modelling and was far removed from operational applications.

9.15 Under Li's guidance, Wu began transferring classified documents on radar systems and stealth technologies. The operation's tradecraft relied on encrypted communications for day-to-day interactions, while document transfers were conducted through secure cloud storage links. Li ensured that Wu remained comfortable with the process, emphasising professionalism and financial reward.

9.16 By early 2010, Wu's expanded role at Lockheed Martin granted him access to proprietary information about the AN/APG-77 radar. Li capitalised on this development, tasking Wu with specific requests for technical documents, including blueprints, stealth optimisation algorithms, and radar performance data.

9.17 To minimise risks, Li arranged for all transfers to occur via dead drop and encrypted messaging service Signal. Payments for each transfer were increased substantially, reinforcing Wu's commitment. Olvana's cyber division worked in parallel to integrate Wu's contributions into their broader espionage efforts. The data provided critical insights into radar cross-section management and signal processing techniques, directly informing the development of the J-20 stealth fighter. By the time of its unveiling in 2011, the J-20 displayed capabilities strikingly similar to those of the F-22.

Discovery and arrest

9.18 In late 2011, U.S. counterintelligence capabilities detected irregular data access patterns within Lockheed Martin's systems. A forensic audit revealed that Wu had accessed files unrelated to his direct responsibilities. Concurrently, his financial records were flagged for significant cryptocurrency transactions inconsistent with his known income.

9.19 By early 2012, Wu was placed under active surveillance. Investigators identified his communications with Li, including encrypted emails and file transfers. On March 15, 2012, Alex Wu was arrested at his home in San Francisco. A search uncovered a laptop containing classified material, transaction records of cryptocurrency payments, and correspondence with Li.

9.20 Li, operating under a false identity, disappeared shortly before Wu's arrest and remains untraceable. Her role as the central HUMINT operative in the operation was confirmed during Wu's interrogation.

Impact of the Operation Silent Spectrum

9.21 The compromised information from the success of Operation Silent Spectrum included:

a. Detailed blueprints and operational parameters of the AN/APG-77 radar.

b. Software algorithms critical to the radar's ability to detect targets while maintaining stealth.

c. Advanced materials data related to radar absorbency and signal management.

9.22 Olvana's accelerated development of its J-20 fighter is widely attributed to the stolen AN/APG-77 data. Analysts observed striking similarities in the J-20's radar capabilities and stealth characteristics, suggesting a direct lineage to the compromised U.S. systems.

9.23 In 2013, Wu pled guilty to charges of espionage and conspiracy. He was sentenced to 27 years in federal prison. Wu's motivations were revealed during the trial which were a combination of financial desperation and a belief that his actions were low risk to the security of US DoD.

Section 9-3. Honeypot – Operation Crimson Veil

9.24 Operation Crimson Veil is one of Australia's most advanced honeypot espionage operations orchestrated by the Olvanan MNS. The operation targeted the infantry fighting vehicle (IFV) program involving MAJ Ethan Bradley, a senior technical officer involved in the IFV's targeting system development. Through a meticulously planned honeypot strategy, the MNS exploited Bradley's personal vulnerabilities, including marital discord and a secret life of infidelity, to extract classified information.

9.25 The MNS began identifying potential targets within the IFV program shortly after its announcement as a pivotal component of Australia's future defence strategy. Using social media and professional networks such as LinkedIn, MNS operatives compiled a list of personnel with access to sensitive aspects of the program. Bradley emerged as a promising target due to his role in developing the vehicle's advanced targeting system and his extensive public-facing digital footprint.

9.26 Further investigations revealed a strained personal life. Bradley's private profiles on multiple dating apps, which he used despite being married, indicated a pattern of infidelity. Posts and interactions on these platforms, along with publicly accessible metadata, highlighted his continual engagement in secretive and passionate encounters. This vulnerability marked him as a prime candidate for exploitation.

9.27 In early 2019, an MNS operative operating under the alias 'Libby Wong' (see Figure 9.6) approached Bradley through a niche professional networking platform focused on defence technology. Presenting herself as an European defence consultant with expertise in battlefield systems, Libby initiated conversations about Bradley's work and the challenges of military innovation.

9.28 Over several months, their discussions moved from professional exchanges to more personal topics. Libby skilfully leveraged Bradley's frustrations with his personal life, providing an empathetic ear to his complaints about his failing marriage. Their exchanges became increasingly intimate, with Libby portraying herself as someone who 'understood' him in ways others did not.

9.29 By mid-2019, Libby proposed an in-person meeting during an international defence technology symposium in Singapore. The rendezvous was framed as a professional networking opportunity but quickly evolved into a romantic and physical relationship. This marked the beginning of a calculated effort by the MNS to entwine Bradley emotionally and physically with Libby.

9.30 Throughout 2020, Libby deepened her connection with Bradley. The couple frequently met under the guise of business trips, with encounters taking place in high-end hotels across Southeast Asia and Europe. Each meeting reinforced the bond between them, blending romance and passion with a shared interest in defence technology.

9.31 Encrypted communication became their primary means of maintaining contact. Using secure messaging applications, Libby began subtly probing Bradley for insights into the IFV program. At first, these inquiries were framed as innocent curiosity, but over time, they grew increasingly pointed. She emphasised her admiration for his expertise and made him feel valued in ways his personal life did not.

9.32 To ensure secrecy, Libby coached Bradley on how to conceal their relationship. She provided him with an encrypted device for their exchanges, which Bradley rationalised as a necessary precaution due to their affair and professional discussions of ‘sensitive nature’.

9.33 By early 2021, Bradley had become fully ensnared in the operation. Libby, now positioned as his confidant and lover, persuaded him to share classified information about the IFV’s targeting system. Her approach was calculated, appealing to his ego and suggesting that his insights would help her ‘shape the future of defence systems.’

9.34 Bradley began providing detailed descriptions of the system’s capabilities, vulnerabilities, and unique features, transmitting the information through encrypted messages. The MNS used this intelligence to significantly advance their understanding of next generation targeting systems, directly benefiting Olvana’s military development.

9.35 In late 2022, irregularities in Bradley's behaviour and unexplained absences during critical project phases drew the attention of Australian security agencies. Routine monitoring of internal communications and personnel flagged encrypted messaging activity and unexplained foreign travel as potential red flags.

9.36 Further investigation revealed a pattern of interactions with 'Libby Wong,' whose identity could not be corroborated through official records. Surveillance and digital forensics uncovered Bradley's use of the encrypted device and detailed logs of their exchanges. In November 2022, Bradley was confronted during a security interview, during which he confessed to the affair but initially denied sharing classified information.

9.37 Forensic analysis of his devices provided irrefutable evidence of his transmissions to Libby, leading to his arrest in December 2022. Libby, operating under a false identity, vanished without a trace, leaving behind no digital or physical footprint.

Figure 9.6: Surveillance image of suspected Ministry of National Security agent, Libby Wong

Impact of the Operation Crimson Veil

9.38 The MNS successfully extracted critical details about the IFV's targeting system. While the full extent of the compromise remains classified, analysts believe the information provided a significant edge in developing countermeasures and rival systems.

9.39 The breach resulted in a major review of personnel vetting processes within Australian defence projects. Public confidence in the IFV program's security was shaken, delaying its deployment and increasing scrutiny of similar initiatives.

9.40 Bradley was charged with espionage and breach of national security laws. During his trial in 2023, he expressed remorse, attributing his actions to emotional manipulation and personal failings. His lawyers have entered an appeal on his 15-year sentence.

Section 9-4. Assassination

9.41 Senior Colonel Zhao Ming held a position of considerable influence within the OPA, particularly in the development of sophisticated cyber-warfare capabilities and oversight of secret weapons programs. Over time, he grew increasingly troubled by systemic corruption at the highest level of power and subjugation to a totalitarian government. Fearing retaliatory measures if he attempted to expose these activities internally, Ming instead opted to defect in pursuit of asylum in 2023.

9.42 Anticipating heightened airport surveillance, he was provided a covert maritime route to escape Olvana, boarding an unmarked vessel from a secluded coastal region under the cover of darkness. This vessel made a brief, clandestine journey through international waters before transferring Ming to a neutral port, from which he travelled to the United States. Once in the United States, he commenced debriefing sessions with U.S. intelligence officials, revealing crucial details about Olvana's defence infrastructure, future weapons research programs and military command structure. As part of his defection efforts, Senior Colonel Zhao Ming was afforded a new identity, Brendan Xi and allowed to settle in the US (see Figure 9.7).

Figure 9.7: Social media image of Brendan Xi, formerly Senior Colonel Zhao Ming of Olvanan People's Army

9.43 Olvana's leadership deemed these revelations a severe threat to national security. Fearing the potential exposure of further sensitive information, MNS authorised an elimination mission designed to minimise forensic evidence and maintain plausible deniability.

9.44 Ming's in-depth knowledge made him intimately familiar with classified projects, specific cyber-warfare assets, and key vulnerabilities within Olvana's military apparatus. Public disclosure of these details risked inviting diplomatic sanctions or military countermeasures from adversarial states. There was also concern

that Ming's successful escape would inspire similar actions among disillusioned officers. Given these stakes, Olvana's internal security apparatus elevated Ming's elimination to a top-priority directive.

9.45 The first operational challenge was locating Xi in a plethora of potential hideouts. Traditional espionage proved ineffective, given the vigilance of U.S. security agencies that were intent on protecting Xi as a high value intelligence asset.

9.46 However, during February of 2024, a rare opportunity presented itself where Xi had agreed to deliver a keynote speech on cyber defence at a prominent security forum in Washington, D.C. The event offered a controlled venue—albeit one with layered security, media attention, and VIP attendees from across the globe. For MNS, it also promised a singular chance to strike in public, sending a resonant message that no traitor would ever be safe should they defect.

9.47 The assassination plan relied on two principal elements:

a. Covert infiltration of the event's digital systems via sophisticated malware.

b. Physical sabotage of the AV equipment used by conference speakers.

9.48 Well before the event, the assassination team deployed a potent malware suite known as Nightcrawler. Operatives introduced Nightcrawler into the symposium's online registration portal through a seemingly benign software patch. Once installed, Nightcrawler accessed the guest list, camera systems, and digital identity checks for all attendees. As the date of the conference neared, Nightcrawler transmitted real-time updates on every individual who passed through the venue doors. Its critical function, however, was facial recognition that would confirm Xi's identity with near-instant precision the moment he checked in to the event.

9.49 Simultaneously, another Black Horizon cell moved to compromise the event's audiovisual preparations. Posing as legitimate crew members from a reputable AV company, they managed to conduct a routine 'equipment inspection' the night before

the symposium. Under the guise of testing microphone outputs, these operatives replaced Xi's designated headset with a near-identical device containing a miniature shaped charge.

9.50 The sabotage was carefully concealed within the microphone's casing, where the explosive components were camouflaged by typical audio wiring. Even if the gear had undergone extra scrutiny, operatives ensured their modifications appeared indistinguishable from standard parts.

9.51 On the morning of Xi's speech, uniformed security teams performed last-minute sweeps, while staff busied themselves seating foreign diplomats, defence experts, and media professionals. Xi, accompanied by a modest security detail, arrived as conference organisers hurriedly fitted him with the prepared headset, ensuring he sounded crystal-clear for the global live stream that would broadcast his address to a digital audience.

9.52 Within minutes, Nightcrawler registered Xi's profile, matching his face against stored biometric data gleaned from decades of public and classified Olvanan records. An operative monitoring Nightcrawler's feed gave final confirmation that the target was in place, microphone wired, and system connections secured.

9.53 Upon Xi's commencement of his address, audio-visual recordings confirm that he began speaking into a headset equipped with a concealed shaped charge. This device had been covertly modified prior to the event by an Olvanan operative. Shortly after Xi took the stage, Nightcrawler software verified his identity by matching facial recognition data against preloaded records. Once the match was confirmed, a wireless signal labelled 'Initiate' was transmitted to the operative's pocket receiver. The operative activated the shaped charge in the headset via a concealed switch.

Figure 9.8: Xi preparing to deliver his keynote speech moments before his assassination

9.54 The resulting detonation fired a small and concentrated blast of shrapnel into the side of Xi's head, causing immediate fatal injuries. The event was recorded by on-site journalists and attendees, and it prompted widespread panic within the auditorium. Observers reported that multiple individuals took cover or attempted to exit the venue in the immediate aftermath.

9.55 Initial investigations of the scene indicate that the headset and its internal components were largely destroyed by the blast, leaving minimal forensic evidence as to the origin or specific composition of the shaped charge. Further analysis is ongoing, but no publicly disclosed findings have definitively linked the operation to Olvana or its clandestine units.

9.56 The blast that caused Xi's untimely death drew immediate intervention by venue security and on-site medical personnel. Despite prompt assistance, Xi exhibited no signs of recovery, and paramedics pronounced him deceased at the scene. Local authorities and federal agents arrived shortly after, sealing the premises for forensic examination. Investigators discovered indications of a shaped charge detonation integrated into the audio equipment. Minimal fragments remained to guide further inquiry, suggesting a high-level of precision in the device's construction and concealment. Electronic records from the event's security systems had also been compromised, erased by an advanced malware leaving the critical timeline of events obscured.

9.57 Media outlets, both domestic and international, quickly referred to the incident as 'a brazen act of international intrigue,' whilst official statements from Olvana condemned 'all forms of political violence' without specifically addressing the circumstances of Xi's death. Unconfirmed reports have speculated the assassination was conducted by Black Horizon. These allegations remain speculative; no verifiable evidence has emerged to conclusively link Black Horizon to the operation.

This page intentionally blank

Abbreviations

The source for approved Defence terms, definitions and abbreviations is the Australian Defence Glossary (ADG), available on the Defence Protected Network at http://adg.dpe.protected.mil.au/.

Opposing Forces (OPFOR) abbreviations are specific to enemy publications and will not be found in the ADG.

AESA	Active Electronically Scanned Array
DSL	Data Security Law (OPFOR)
CODSIT	Central Office for Defence, Science, Industry and Technology (OPFOR)
EV	electric vehicle
GSD	General Staff Department (OPFOR)
GOCO	Global Outreach and Coordination Office (OPFOR)
HUMINT	human intelligence
IFV	infantry fighting vehicle
MNS	Ministry of National Security (OPFOR)
OCP	Olvanan Communist Party (OPFOR)
OCP	Olvana Central Party (OPFOR)
OI26	Olvana Innovates 2026 (OPFOR)
OPA	Olvanan People's Army (OPFOR)
PEIB	Political and Economic Intelligence Bureau (OPFOR)
PRO	People's Republic of Olvana (OPFOR)
SHC	Supreme High Command (OPFOR)
SOE	State Owned Enterprise (OPFOR)
SOE	State Owned Entities (OPFOR)
SPF	Special Purpose Forces (OPFOR)
UFWD	United Front Work Department (OPFOR)

This page intentionally blank