JAIPUR NATIONAL UNIVERSITY
ADDRESS: JAIPUR - AGRA BYPASS, NEAR NEW RTO OFFICE, JAGATPURA, JAIPUR. PH. 0141-7197070

THE KINGDOM OF ELDORIA

V.

THE REPUBLIC OF VAROSIA

1. The Kingdom of Eldoria and the Republic of Varosia are two neighbouring sovereign nations which are located near a growing digital trade corridor. According to the World Trade Organisation (WTO) regional economic statistics, this corridor will contribute about 18% of the total GDP of both countries by 2023. The dependence of both states on cyber-enabled trade and finance is evident in the fact that 45% of Eldoria's cross-border online banking operations pass through server hubs in Varosia. At the same time, 37% of Varosia's blockchain-based data transfers rely on fintech APIs licensed by Eldoria's regulatory authorities. This interdependence is often described as the "cyber-silk artery" of trans-Eurasian trade, and for its development, more than USD 220 billion was invested in digital infrastructure in both States from 2015 to 2023.

2. Despite strong economic ties, the relationship between Varosia and Eldoria has always been predicated on strategic concerns, especially when it comes to cybersecurity. In 2023, Varosia and Eldoria ranked at 46 and 51 out of 145 states, respectively, in the annual Global Cybersecurity Trust Index. At the same time index flagged them as "manual cyber risk hotspots" due to overlapping legislative gaps and a lack of prospects for intergovernmental cooperation. Though both States regularly raise the cyber sovereignty principles of the Tallinn Manual in parliamentary discussions, there remain issues of jurisdiction and accountability, as they have never been incorporated in a reciprocal agreement. When Central Bank of Eldoria disclosed a cybersecurity breach involving unauthorised rerouting of over USD 1.5 billion on February 14, 2024, the problem was aggravated, which represented almost 12 % of the sovereign wealth fund set aside for infrastructure development as part of its "Vision 2030" economic plan. According to the Interpol Cyber Threat Report 2024, the illicit funds were channelled through at least nine

different cryptocurrency wallets located in Asia, Eastern Europe, and Latin America. It was subsequently anonymised utilising mixing servers, which had a projected 96% efficacy at concealing transactional trails.

3. The ransomware strain used in the cyber-attack was subsequently named “HydraLock-24.” The Cybersecurity Ventures Report 2024 states that it has already been associated with global financial sector losses of over USD 6.4 billion. In addition to being a financial loss for Eldoria, the government saw the breach as a lasting damage to its sovereign right to defend vital national resources. Due to a credibility shock, international rating agencies downgraded Eldoria's sovereign wealth fund by 2.5 points on the Global Fiscal Stability Index, which was valued at USD 12.7 billion in 2023.

4. An immediate probe was launched by Eldoria's National Cyber Security Agency (NCSA). The forensic investigations identified servers located in Varosia as the source managed by NetSecure Ltd., an internet infrastructure company, registered in Varosia with clients in 31 countries and a daily traffic volume of roughly 8.3 petabytes. Malware traces found in forensic data were matched with the cybercriminal syndicate "Dark Hydra," which was linked to at least 27 significant ransomware incidents from 2019 to 2023, including one that cost the South Atlantic Monetary Fund more than USD 4.1 billion. The Eldoria intel agency had already alerted the public of Dark Hydra's operational base in Varosia in the 2023 Annual Cyber Threat Bulletin. According to Eldoria, Varosia allegedly violated the concept of due diligence in cyberspace by failing to implement appropriate enforcement measures despite the alerts. This has been discussed in experts' forums and frequently implemented by governments since the 2015 consensus report of the United Nations Group of Governmental Experts (UNGGE).

5. The Eldorian Government issued a public statement based on forensic observations that Varosia permitted activities on its territory that explicitly infringed upon Eldoria's sovereignty. Eldoria's president, citing Article 2(4) of the UN Charter, called the operation an "act of cyber aggression" while comparing it to the cyber equivalent of a hostile military act. Following this, Eldoria outlawed the use of Varosian digital platforms, imposed sanctions on 15 Varosian banks and technology companies unilaterally, and froze USD 620 million worth of assets. This development

disrupted 22% of transnational digital payments in the region.

6. In furtherance of the aforesaid contentions, Varosia firmly rejected any accountability, and the Ministry of Foreign Affairs stressed that the simple assertion that servers were present within its territorial limits could not establish State culpability or prove attribution. Further, Varosia claimed that entities acting from afar and beyond the jurisdiction of the State had also compromised NetSecure Ltd's infrastructure. Eldoria's actions were condemned by the Varosian administration as financial extortion that violates WTO regulations. Varosia contended that Eldoria was obliged by the General Agreement on Trade in Services (GATS). Furthermore, Varosia argued that a clear concept of "cyber aggression" had not yet been established by international law. They argued that the issue should be categorised as international organised cybercrime rather than an act attributable to the State.

7. Despite diplomatic protests, Eldoria's Supreme Court worsened the situation by issuing arrest warrants against the Varosian national CEO of NetSecure Ltd. for their complicity in cyberterrorism. Eldoria called for his extradition under the Budapest Convention on Cybercrime, 2001. Varosia, however, denied the motion, stating that its legal system does not include dual criminality and that widespread cyber-attacks are treated as "economic fraud" rather than "cyberterrorism," as defined under Eldorian law. Varosia contended that extradition under such conditions would undermine its sovereignty and violate its citizens' constitutional rights.

8. The Attorney General of Eldoria argued that cybercrimes of this gravity should be penalised wherever the offenders are located, by citing precedents from the Princeton Principles on Universal Jurisdiction (2001). Additionally, Economic cybercrime is not covered by universal jurisdiction under customary law, which is limited to the "most serious crimes of concern to the international community," such as piracy, war crimes, and genocide, according to Varosia, who rejected this as an illegal extraterritorial expansion of jurisdiction. This issue unfurled quickly around the world. Eldoria claimed that the incident jeopardised global security and peace and asked the UN Security Council to convene an emergency meeting in March 2024. Nevertheless, draft resolutions calling for Varosia to help with enquiries were vetoed by two permanent members. Collectively, the two nations invested more than USD 35 billion in Varosia's digital

infrastructure. Eldoria thereupon initiated proceedings before the International Court of Justice (ICJ) in April 2024.

9. Eldoria claimed that Varosia had violated its duties under international law by neglecting to stop destructive cyber activities originating from its soil, thereby violating its territorial integrity and sovereignty. In addition, Eldoria demanded USD 1.5 billion in reparations with interest, along with declarations affirming that its measures were legitimate countermeasures. Varosia was also accused of failing to cooperate under the Budapest Convention, even though it was a signatory. Varosia, however, filed preliminary objections, arguing that the ICJ lacked competence since the matter concerned criminal law enforcement and was outside the purview of state authority. Furthermore, Varosia contended that in the absence of any proof of State control, there is no imperative customary law requiring States to stop all cyber operations coming from their territory. Furthermore, it claimed that Eldoria's unilateral sanctions violated WTO agreements by constituting illegal countermeasures and that its stipulations under the Budapest Convention relieved it of certain cooperation obligations.

10. Varosia claimed that Eldoria's application was invalid since it was submitted maliciously. According to Varosia, who relied on declassified intelligence data, Eldoria carried out a cyber operation against its energy infrastructure in 2022 under the guise of "Project Falcon," causing only minor disruptions. Eldoria described the operation as a defensive penetration exercise. Eldoria's sovereign wealth fund suffered losses that forced the cancellation of four major infrastructure projects, including the USD 2.3 billion East River Smart City. Within three months of the breach, the Eldorian government's public popularity ratings fell by 17%. Eldoria's sanctions destabilised the fintech markets in Varosia, leading to an 11% drop in its Digital Index Fund and an enormous domestic outcry over alleged foreign intimidation. Although bilateral trade reached USD 42 billion in 2022, it fell by 23% in 2024. As a result, in the rapidly evolving field of international cyber law, the dispute has become one of the most important issues before the ICJ.

11. Despite years of mutual reliance on technology and the economy, the Republic of Varosia and the Kingdom of Eldoria are currently embroiled in one of the most significant cyber law cases ever heard by an international tribunal. Regardless of their concerns about admission, both

countries have accepted compulsory jurisdiction of the International Court of Justice under Article 36(2) of the statute. Upon preliminary consideration, the Court admitted the case and confined its examination to questions relating to jurisdiction, sovereignty, State responsibility, and international legal obligations in cyberspace.

12. The proceedings were instituted on February 14, 2024, following the HydraLock-24 Cyber attack, which resulted in a loss of USD 1.5 billion to the Eldorian Sovereign Wealth Fund due to random demands and subsequent cryptocurrency transfers designed to obscure the transactional trail. Investigators of the National Cyber Security Agency in Eldoria discovered that the breach was associated with a server of NetSecure Ltd. , which was an infrastructure service provider in Eldoria. The agency further suspected that the server may have been linked with Dark Hydra, in pursuance of which, the President of Eldoria invoked Article 2(4) of the UN Charter and referred to the incident as an "act of cyber aggression."

13. On the one hand, Eldoria maintains that its actions were appropriate and consistent with its obligations under Article 22 of the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). Contrarily, Varosia does not accept that the sanctions constitute a legitimate exercise of authority and argues that they are viewed as an illegal form of economic coercion in breach of the WTO principles of non-interference. As indicated in official WTO statistics, the number of trade-related cyber disputes increased by 56% from 2017 to 2023, underscoring the widespread implications of current cyber disputes. The procedures are further hampered by charges of reciprocal misbehaviour. According to Varosia, Eldoria engaged in offensive cyber operations through "Project Falcon" in 2022, which were allegedly aimed at its electricity grid.

14. There have been serious political and financial repercussions. Eldoria's GDP shrank by 1.8% in 2024 due to asset losses from sovereign wealth funds, delaying significant infrastructure projects. Eldoria's sanctions led to a 14% drop in foreign investment in Varosia's technology sector, which fuelled demonstrations at home and eroded investor confidence. With projections of cyber-crime to generate USD 10.5 trillion in global damages by 2025, it will have an effect on both the parties involved (Eldoria and Varosia) as well as on the anticipated development of international cyber

law.

15. Thus, this Tribunal is faced with these questions:

1. Whether this Tribunal has the authority to adjudicate issues related to international cyber actions.
2. Whether the alleged cyberattack breached the sovereignty or territorial integrity of Eldoria.
3. Whether the Republic of Varosia can be held internationally responsible for cyber operations conducted by non-state actors on its territory pursuant to international law and treaty obligations.
4. Whether Eldoria is entitled to a remedy or reparation under international law, including the law of state responsibility.

Note:

** The Kingdom of Eldoria, by virtue of various international human rights treaties, is hereby considered a party to international law for the purposes of this case by the Republic of Varosia (Varosia); and,*

** The participants may include as sources of international law besides conventions and treaties, other legally binding forms of international law.*