University of the Sunshine Coast

Student: Torin Flanagan 1169130

Course Coordinator: Dr Declan Humphreys

Submission Due Date: 09/06/2025

SEC302 Ethics in digital investigation and cybersecurity

Assessment Task 3: Ethical Decision-Making In Cyber Security

**Ethical Decision-Making in Cyber Warfare (Part 1)**

I acknowledge the use of ChatGPT in this assessment.

I confirm that the extent of the use of AI in this assessment is limited to the conditions specified above.

**Identification and Evaluation of Ethical Issues**

The ongoing cyber conflict between Veridia and Torvus poses high risks and the potential for disproportionate harm.

Though Torvus initiated attacks, they may underestimate Veridia’s capability to target critical SCADA systems like dams and power grids, posing severe risks to critical Torvus civilian infrastructure. Torvus’ offensive posture likely leaves many hidden vulnerabilities. If Veridia shift its National Cybersecurity Agency (NCA) to offence, nation defences will weaken, increasing exposure to further attacks. Similar to the Russia-Ukraine conflict, failed countermeasures may erode public trust and escalate tensions into physical warfare. Involving private Veridian hackers could backfire, as Torvus may exploit access and turn Veridia’s own “DustR” worm against it.

Veridia faces two poor options; launching a pre-emptive strike risks civilian casualties, escalation, and weaker defences, while restraint preserves defences but increases vulnerability for Torvus to further pursue attacks.

This is a national issue that goes far beyond legality or tactical efficiency. Even if lawful, a pre-emptive strike raises ethical concerns around civilian harm, proportionality, unintended consequences, and long-term instability. Ultimately, moral judgement must guide Veridia’s response.

**Relevant Facts From The Case Study**

*Relevant facts from Veridia vs Torvus cyber conflict:*

* Veridia upholds international law while Torvus does not.
* Torvus’ elite unit “FrostBug” plans to breach Veridia’s energy networks.
* Torvus attacks threaten widespread blackouts and national instability.
* Veridia knows of SCADA vulnerabilities in Torvus infrastructure.
* NCA is split on launching a pre-emptive strike.
* Veridia has strong expertise but limited resources.
* Intelligence suggests targeting a Torvus sector tied to military bases, but impacts civilians, hospitals, and businesses.
* Offensive focus would weaken Veridia’s defences.
* Private hacking groups may support the NCA; one developed “DustR’, a spreadable system-locking worm.

*Meanwhile, unknowns include:*

* Scale, timing, and impact of Torvus cyberattacks or escalation to physical warfare.
* Civilian and national consequences of mutual cyberattacks.
* Whether a pre-emptive strike would deter future attacks.
* Reactions from neighbouring nations.
* Legal basis for Veridia’s potential offence.

*Stakeholders:*

* Veridia’s civilians, government, military, NCA, and private hackers.
* Torvus’ civilians, government, and military.
* Civilians on both sides face the highest risk of being most affected.

*Possible options for action:*

* Launch a targeted pre-emptive strike on Torvus military systems.
* Execute a broader cyber offensive operation despite civilian risks.
* Strengthen Veridia’s defences and avoid escalation.
* Attempt diplomacy; if ignored, issue a public warning.
* Seek advice from ethics boards and allied nations.

Veridian government and NCA lead decision-making, but broader consultation is limited. Creative alternatives like targeted deterrents may help de-escalate while protecting national interests.

**Applicable Professional Codes of Ethics And Legal Requirements**

*UN charter article 2(4):*

Under Article 2(4) of the UN Charter (1945), cyber responses remain legally grey due to attribution challenges. However, Veridia has confirmed Torvus’ involvement in cyber intrusions. Given Torvus espionage, intelligence gathering, and pre-emptive cyber operations, the threat of force is imminent, providing Veridia legal grounds to act under international law (Waxman, 2011).

*International humanitarian law (IHL):*

IHL applies when cyber operations link to actual or expected armed conflict (European Commission, 2024). It protects civilians and critical infrastructure from harm. Veridia’s credible intelligence suggest Torvus’ actions meet this criteria, particularly through disruptive attacks on infrastructure. Veridia must respond using IHL principles; distinction, proportionality, and precaution to ensure ethical conduct (Diamond, 2014).

*Veridian national laws:*

Torvus’ actions violate nation laws on cybersecurity, data protection, privacy, cybercrime, and intelligence acts. A legal framework similar to Australia’s Cyber Security Act 2024 (Australian Government, 2024) enables defence against such cyberattacks. Torvus breaches laws akin to the GDPR (Butera, 2018), the 1988 Privacy Act (Federal Register of Legislation, 2019), and Australia’s Cybercrime Act (Attorney-General's Department, 2022). Intelligence laws similar to Australia’s Defence Intelligence Act (Australian Government Defence, 2024) would support counterintelligence operations. In summary, Torvus clearly violates multiple national laws.

*Professional obligations and standards:*

Bodies like ACM (2019) and IEEE (2018) set ethical standards; transparency, proportionality, and civilian protection. Veridia’s NCA, if operating under professional charters, is likely bound by similar standards. Cybersecurity obligations align with the Australian Signals Directorate (2025) principles, being:

1. Govern – Maintain strong, well-resourced, and accountable NCA.
2. Identify – Monitor assets and assess threats.
3. Protect – Apply appropriate safeguards to risks.
4. Detect – Identify and analyse cyber threats.
5. Respond – Mitigate and recover from cyberattacks.

**Evaluate Alternative Actions Using Moral Principles and Theories**

1. *Utilitarianism –* The ethical path maximises benefits while minimising harm. Veridia should strengthen defences and pursue diplomacy to protect civilians, infrastructure, and reduce invasion risks (Christen et al., 2020).
2. *Deontology –* Veridia has a duty to protect citizens, uphold law, and avoid harming innocents. A broad pre-emptive strike breaches non-combatant immunity and violates moral obligations (Christen et al., 2020).
3. *Virtue ethics –* Veridia must act with prudence, justice, temperance, and courage in upholding moral choices under pressure. Choosing diplomacy and defence over retaliation reflects moral integrity and national values (Christen et al., 2020).
4. *Rights-based ethics* – A pre-emptive strike risks violating Torvus civilians’ rights to life and safety. Veridia must prioritise precision, proportionality, and human dignity over national interest (Christen et al., 2020).
5. *Autonomy* – Citizens have the right to live freely and access essential services. Veridia must minimise disruption and prioritise defence over violence to respect individual autonomy (Christen et al., 2020).
6. *Common good/beneficence* – National stability and safety are key. Veridia should protect infrastructure, prevent panic, and seek support, avoiding escalation and counterattacks (Christen et al., 2020).
7. *Justice* – Fair treatment is essential. Veridia must target aggressors, not civilians, and distribute risks ethically. A limited, justified response will align with this principle (Christen et al., 2020).
8. *Non-maleficence* – Avoiding harm is vital. Escalation risks widespread damage. Defensive strategies and containment better uphold this principle than offensive actions (Christen et al., 2020).
9. *Just War theory* – A Christian ethical framework, Just War theory guides nations on when and how to engage in conflict morally. It doesn’t justify war but limits it to exceptional cases, encouraging peaceful alternatives. The theory holds that while all war is evil, a 'just war' may be the lesser evil. It includes two key parts: jus ad bellum (when the conditions for war are deemed justifiable) and jus in bello (the most ethical approach for the situation). For Veridia’s actions to qualify as a ‘just war’, its government and NCA must ensure the cyber conflict with Torvus is both a justified response and carried out as the most ethically moral option (BBC, 2014).

**Chosen And Tested Option For Action**

In responding to predicted cyber conflict from Torvus, Veridia’s most ethical and effective course of action is to combine utilitarianism with the Just War theory. This dual-framework approach ensures Verdia’s actions maximise overall benefit while minimising harm to both its population and innocent Torvus civilians. Additionally, by applying the Just War theory, Veridia ensures that any potential retaliation remains morally and legally justified.

Utilitarianism supports decisions that protect the majority, avoid unnecessary harm, and promote the greatest good. For Veridia, this means prioritising civilian safety, infrastructure security, and well-informed actions based on verified intelligence regarding Torvus intentions. It encourages a measured, defensive response that minimises risks while preserving nation stability.

The Just War theory ensures that any use of force is only considered when all peaceful alternatives are exhausted. It requires clear justification for conflict, proportionality in response, and a strict focus on legitimate military targets. Therefore, this theory keeps Veridia’s actions ethical, restrained, and aligned with international standards.

*Recommended actions to perform under this dual-framework include:*

* Strengthen Veridia’s cyber defences, especially around critical infrastructure (e.g. hydroelectric dams and substations).
* Issue a public deterrent message to Torvus outlining consequences from continued cyber hostility.
* Open backchannel diplomacy to reduce tensions and explore peaceful resolutions.
* Continue intelligence gathering to further assess Torvus’ ongoing cyber operations.
* Prepare a proportionate and targeted cyber counterattack plan to be executed only if aggression escalates further.

*Utilitarian outcomes achieved:*

* Protection of innocent civilians from both nations.
* Avoidance of full-scale warfare and escalation.
* Preservation of Veridia’s critical systems and internal stability.
* Time gained for intelligence gathering and better strategic decisions.

*Ethical outcomes through Just War theory:*

* A pre-emptive cyberattack is currently unjustified due to lack of conclusive evidence.
* Avoids disproportionate harm and prioritises ethical conduct.
* Ensures all peaceful alternatives are pursued first.
* Actions focus on nation defence, not revenge or political gain.
* Any military response must comply with legal, ethical, and international standards.
* Targets are limited to verified military or cyber assets only.

*Conclusion:*

By applying both utilitarianism and Just War principles, Veridia adopts a balanced and morally defensible approach. It ensures that if conflict occurs, it is justified, proportionate, and strategically necessary. This dual-framework strengthens Veridia’s defence, maintains its international credibility, and maximises public support by protecting lives, values, and national integrity.

**Veridia’s Cybersecurity Response (Part 2)**

With Torvus continuing its persistent cyber aggression, Veridia stands firm in committing to ethical, lawful, and responsible responses. Our NCA team have created a strategy using a globally accepted dual-framework, being utilitarianism partnered with the Just War theory, to guide all decisions towards public safety, legal integrity, and global stability.

A top national priority is protecting citizens and critical infrastructure. Through focusing on defence, intelligence gathering, and pursuing diplomacy channels with Torvus, we aim to reduce threats while maintaining public trust and nation stability. This approach upholds utilitarian values by maximising overall benefit and minimising harm to both parties.

Cyber countermeasures will only be considered if absolutely necessary, and only after all peaceful alternatives are exhausted. The Just War theory ensures any Veridian response remains proportionate, targeted, and legally justified in response to actions conducted by Torvus.

Veridia is not to act with retaliation but instead through strategic care, ethical integrity, and plausible respect to human rights. Because of this principled and moral approach, we persist to work with internal and possible international partners to deter greater aggression and preserve peace inside the digital domain.

**References**

* ACM. (2019). Association for Computing Machinery. Acm.org. https://www.acm.org/
* Attorney-General's Department. (2022). Cybercrime. Attorney-General’s Department; Australian Government. https://www.ag.gov.au/crime/cybercrime
* Australian Government. (2024). Federal Register of Legislation - Cyber Security Act 2024. Legislation.gov.au. https://www.legislation.gov.au/C2024A00098/asmade/text
* Australian Government Defence. (2024). Intelligence controls. Defence.gov.au. https://www.defence.gov.au/about/governance/intelligence-controls
* Australian Signals Directorate. (2025, March 18). Cybersecurity principles. Australian Government. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-principles
* Butera, G. (2018). General Data Protection Regulation (GDPR): What’s in it for Australian organisations? In Nixora Group. https://www.dfat.gov.au/sites/default/files/nixora-group-eufta-submission.pdf
* Christen, M., Gordijn, B., & Loi, M. (2020). The International Library of Ethics, Law and Technology 21. https://library.oapen.org/bitstream/handle/20.500.12657/22489/1/1007696.pdf#page=88
* Diamond, E. (2014). Accept Terms and Conditions on JSTOR. Www.jstor.org. https://www.jstor.org/stable/pdf/resrep08957.8.pdf
* European Commission. (2024). International Humanitarian Law. Civil-Protection-Humanitarian-Aid.ec.europa.eu. https://civil-protection-humanitarian-aid.ec.europa.eu/what/humanitarian-aid/international-humanitarian-law\_en
* Federal Register of Legislation. (2019). Privacy Act 1988. Www.legislation.gov.au; Australian Government. https://www.legislation.gov.au/C2004A03712/2019-08-13/text
* IEEE. (2018). IEEE - The world’s largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE. https://www.ieee.org/
* United Nations. (1945). UN charter. United Nations. https://www.un.org/en/about-us/un-charter
* Waxman, M. (2011). Force. Under UN Charter Article, 2(4), 43–57. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty\_scholarship