The article by Jarvinen, Digital Battlegrounds: Evolving Hybrid Kinetic Warfare explains how the contemporary hybrid warfare incorporates the old ways of kinetic war originated with advanced non-kinetic actions, i.e., cyberattacks on critical infrastructure, telecom or information infrastructures, democratic services, and supply lines. An example given is the October 6-7, 2023 attacks at the onset of the Israeli-Hamas offensive, where hacktivist organisations used DDoS attacks to disrupt the Israeli power grid, missile warning signals were generated through hacked emergency APIs, and other cyber-related sabotage was used with conventional military strikes in a synchronized effort.

These are the acts of violence in the cyberspace and as such, raise the moral questions on whether they abide by Just War principles as part of broader approaches to conflict. Particularly, we should ask: in the face of the justifications of the wider war, can even such cyber operations fulfil the criteria of a just war, or are they unjust even in an otherwise just war?

My claims on the prospects of cyber operation on vital infrastructure in this Case Analysis will be that though the operation might be tactically substantial, utilitarianism proves that it fails to conform to the rules of distinction, proportionality, and immunity of non-combatants making the operation unjust even in the just war.

Part I — Boylan

(a) Central notions faced by Boylan are;

Michael Boylan develops his conception of cyberwarfare by applying the classical theory of Just War (JWT), taking into consideration its adaptations to the special features of the digital war. He contends that the cyber operations ought to be analyzed on whether they involve:

Sabotage, small, regional destabilisations of limited intensity and extent, not amounting to war.

War actions- major, one-time attacks that have great and lasting consequences to the military capacity, the economy and/or safety of a nation.

Boylan underlines that (as opposed to kinetic attacks) cyber operations may be stealthy, deniable, and indiscriminate, which complicate the possibility of adherence to the key requirements of JWT:

Difference: The factors to be attacked and defended are combatants and civilians respectively.

Proportionality: It requires that harm to be caused should be proportional to the military objective.

Necessity: The assault should be militarily essential and need not be attained in a less injurious method.

Sovereignty: The expectation of the rights of either neutral or non-belligerent countries should be adhered to.

Boylan further brings to the fore the issue of proportional retaliation how a state goes about responding morally to cyber aggression without having to unnecessarily escalate it.

(b) Applying Boylan to the case

October 2023 events obviously exceed the category of the mere sabotage. Shutting down or seriously impairing an electricity grid, even temporarily, makes civilian life much more difficult at the systemic level: it may affect, among others, hospitals, emergency response, sanitation, and water flow. Such disruption, by the definition introduced by Boylan, qualifies as an act of war in terms that it has national implications and it disrupts the fundamental societal operations.

The fake alerts of missiles are even more morally problematic. Emergency alert systems have the security of the life of civilians in mind. The consequences of compromising them to conduct a psychological warfare may include mass panic, stampede of the gatherings, and assembling emergency resources in the wrong places. Such implications cause greater harm to civilians in a disproportionate manner rendering the operation to violate JWT principle of distinction.

(c) Utilitarian analysis in the light of Boylan

In the light of utilitarian view, we weigh overall harms and total benefits:

Military advantage: It buys some time to distract or demoralize the opposition population; it may also complicate military coordination.

Harm to civilians: Damage to everyday activity, increased fear and stress, the risks of medical emergencies caused by failures of infrastructure, lack of trust in system of ensuring safety to people.

The regressive implications of such an impact are damages to faith in civil institutions, susceptibility to future propaganda, and lack of resilience in the society. This extensive and sustained civilian casualty is probably more than was any temporary military advantage.

Moreover, the aspect of not needlessly damaging civilian infrastructure is an important addition to the sovereignty principle provided by Boylan: he gives it in the context of a fair war. Proportionality requires utmost care in the sphere of cyber where collateral damage can easily be expanded to other areas; the systems of which they want to attack are very much prominent.

In this way, the attacks in the case analyzed fit in the system described by Boylan and operating under utilitarianism: they are unjust acts of war in effect: against civilian systems, utilizing disproportionate force in terms of the tactical efficiency, and undermining the stability and trust in society.

Part II -Taddeo

(a) Central ideas in Taddeo

Mariarosaria Taddeo questions the sufficiency of conventional JWT to cyberwarfare, which suggests an extended model that would incorporate the knowledge of Information Ethics. She emphasizes:

The Infosphere: The entire environment of information objects, processes and relations. As much as physical infrastructure in modern societies, it is important.

Principle of Information Integrity: Just cyberwar has to safeguard the stability, dependability, and trustworthiness of the Infosphere.

Proportionality in Information Warfare: The effects of action should not cause unnecessary impairment of information systems.

Moral safeguarding of civilian informationola it is important that informational autonomy should be in arms of the civilian so that he or she can make wise decisions and in the case of emergency it is necessary to have information which is true and accurate.

Taddeo holds fast to the determination that cyber-operations should not just be measured in what is physically impacted but also in informational damage furthered.

(b) Applying Taddeo to the case

The sabotage of the Israeli electricity grid and emergency warning systems are negative aspects related to information integrity as far as they directly impact on it. These attacks undermined public confidence in security mechanisms by creating insecurity within the Infosphere by disruping vital services.

Electricity grid attack: In addition to the physical inconvenience created by power cuts, the digital communication system, payment mechanism and data accessibility can be impacted too--bringing cascading system failures in the Infosphere.

False alarms: This actively pollutes the informational environment with the lies instead of the truth, which can save lives. This is a complete denial of informational autonomy since the civilians cease to possess the right to act on credible information.

These are not used against the fighting elements but instead, they take advantage of the reliance of civilians on information systems to provide safety and survival.

(c) The unethical violation is magnified with the help of a utilitarian lens:

Temporary detriments: Panic, injury caused by crowd response, failure of detecting real alerts caused by alert fatigue, disruption of serious services (medical, transportation).

Long-term damages: deterioration of trust in digital systems, resulting in less effective future emergency communications that could result in the loss of lives even following the conclusion of the war.

Advantages: Small, short-term military suitedness due to bewildering and distracting.

The asymmetry is evident i.e. harms greatly exceed benefits. The Infosphere is especially vulnerable as an attack against it is not merely technical; once the trust is gone it takes time to regain it.

Another valuable input in Taddeo s augmented JWT is that although a war may be justified in its own right, the ends are never to be compromised at the expense of the means or rather the civilian lifestyle. The infrastructure and information autonomy of civilians is a moral asset which should not be destroyed. Waging war in disregard of such in order to gain tactical advantages that have minimal impact is not in line with a fair cyberwar.

Conclusion

Cyber warfare like mega DDoSing of power grid systems and micromanaging of emergency systems fits the definition of act of war stated by Boylan, however does not fit the Just War requirements of distinction, proportionality, and necessity. The approach to information ethics that Taddeo presents contributes to this conclusion and demonstrates that such actions undermine Infosphere as well, impairing long-term confidence in crucial systems and lowering informational autonomy of civilians.

Utilitarian calculus could alone show the disasters, civilian suffering, destabilization of the system, breach of trust to be far greater than the momentary military gains. The wider conflict could be justified, but still, these cyberattacks would be illegal actions since they deliberately attack civilian infrastructures and dismantle some vital societal processes.

It can be said that these measures are less harmful in comparison to kinetic attacks resulting into direct bodily killing. Nevertheless, their opportunity costs and systemic adverse effects, particularly the effects on the ability to respond to emergencies, can also be fatal in the long run. Ethical cyber-combat should not exceed our moral authority and still maintain the protection of the non-combatants both in the informational and physical realms.