Cyber Defense in Hybrid Conflict: A Technical, Economic, and Political Dive

15/02/2026

Elie Joe J. Akiki, Cesar Latorre Hernandez, Agustin Plaza de Los Reyes Alvarez, Alberto Martinez Fraile,Michela Salama-Robino, Sarah Maria Y. Chalhoub

Global Strategy Review

Cyber Defense in Hybrid Conflict: A Technical, Economic, and Political Dive

15/02/2026

Editor: Yasmina A. Moussa
Lead Researchers: Elie Joe J. Akiki, Cesar Latorre Hernandez
Senior Researchers: Michela Salama-Robino, Agustin Plaza De Los Reyes Alvarez, Alberto Martinez Fraile, Sarah Maria Y. Chalhoub

Abstract

This report provides a comprehensive analysis of the evolution of modern conflict into the paradigm of hybrid warfare, where traditional boundaries between war and peace have dissolved into a digital "grey zone". It establishes that cybersecurity has shifted from a technical IT concern to a top-tier existential strategic imperative for national defense and global stability. The study examines the mechanisms of this shift across three critical dimensions: technical execution, economic impact, and the resulting legal and political quagmires.

The technical analysis distinguishes between offensive and defensive instruments, highlighting the use of "wiper" malware—such as WhisperGate, IsaacWiper, and Industroyer—designed solely for infrastructure destruction rather than financial gain. The report details the integration of Artificial Intelligence (AI) in automating attacks and generating disinformation, alongside the rise of uncrewed aerial vehicles (UAVs) in coordinated strikes like Ukraine's "Operation Spider's Web". Case studies from the conflicts in Ukraine and Israel-Hamas illustrate how these tools are leveraged to sabotage critical infrastructure and exploit societal vulnerabilities.

A primary contribution of this research is the application of complex economic theories to cyber conflict. The "O-Ring Theory" is utilized to demonstrate how globalized supply chains are only as strong as their weakest digital link; a single cyber blockade can drop the value of an entire production chain to zero. Furthermore, the report identifies a "Reverse Romer" effect, where persistent digital insecurity discourages investment and leads to technological regression. The "Dutch Disease" phenomenon is also explored, showing how nations may over-invest in the "Guns" (military) sector at the expense of the "Butter" (consumer) sector, leading to long-term economic vulnerability.

The final section addresses the crisis of accountability in cyberspace. It analyzes the "attribution problem," where the use of proxies and false flags complicates state responsibility under international law. The application of the Tallinn Manual's rules and the Schmitt Analysis is discussed to determine when a cyber operation constitutes a "use of force". Finally, the report evaluates proactive policy responses, including the EU's NIS2 Directive and NATO's recognition that severe cyberattacks may trigger Article 5 collective defense.

The report concludes that the stability of the international order depends on transitioning from reactive measures to proactive governance. This includes "humanizing" cyber warfare through Geneva Convention-style frameworks and enforcing strict security standards to mitigate the "nuclear curse" of modern technology.

Keywords: Hybrid Warfare, Cybersecurity, O-Ring Theory, Reverse Romer Effect, Dutch Disease, International Humanitarian Law, Tallinn Manual.

Introduction

In the landscape of modern conflict, the traditional boundaries of warfare have entirely dissolved, giving rise to the complex, multi-faceted challenge of hybrid warfare. This profound strategic evolution moves decisively beyond conventional military engagement, seamlessly integrating sophisticated cyber operations, pervasive psychological warfare, and highly organized disinformation campaigns to achieve systemic destabilization without necessitating direct, large-scale kinetic confrontation. This comprehensive report delves into the core mechanisms and pervasive effects of this new security paradigm, establishing a crucial argument: cybersecurity is no longer a mere technical or IT-related concern but a top-tier, existential strategic imperative for national defense and global stability. The ensuing discussion demonstrates precisely how state and non-state actors leverage increasingly advanced digital tools to systematically erode internal national cohesion, fundamentally weaken democratic institutions, and generate systemic uncertainty across all sectors of society. This strategic approach masterfully echoes the ancient principle articulated by Sun Tzu, "defeating the enemy without fighting." Ultimately, this detailed analysis distinguishes between the critical offensive and defensive instruments employed within this combined physical and digital domain, including cyberattack, cyberdefense, uncrewed aerial vehicles (drones), information warfare (disinformation), and psychological operations. This framework provides the necessary foundational structure for both understanding the architecture of and formulating effective countermeasures against the pervasive threats posed by this constantly evolving form of conflict.

I) Technical Interpretation

In the current scenario of international conflicts, the line that separates conventional warfare from cyber operations has become increasingly blurred. The so-called hybrid warfare represents a strategic evolution where traditional military elements are combined with cyberattacks, psychological operations, and disinformation campaigns, all aimed at destabilizing the adversary without the need for direct confrontation. This new form of conflict requires a deep understanding not only of military dynamics, but also of the technical and technological aspects that underpin operations in cyberspace.

Cybersecurity in this context ceases to be an exclusively technical matter to become a top-tier strategic component. Attacking actors deploy advanced tools that can have an immediate impact on national security. Furthermore, disinformation amplified by social networks, bots, and algorithms contributes to eroding the internal cohesion of the targeted countries, generating uncertainty and weakening democratic institutions.

As Sun Tzu wrote in The Art of War, the best way to fight a strong enemy is from within: "Defeat the enemy without fighting."[1] This quote summarizes the essence of hybrid warfare, in which the goal is not the physical destruction of the adversary, but rather their internal weakening through cyber, social, or psychological actions.

In hybrid warfare, the physical and digital domains are combined. The contenders use both offensive and advanced defensive tools. It is therefore appropriate to distinguish between the different tools used: cyberattack, cyberdefense, drones, disinformation, and psychological operations.

Definition and types:

Hybrid warfare is defined as a primarily military strategy that combines different tactics and methods, without disregarding conventional ones. The simultaneous use of both methods offers unprecedented strategic advantages and allows the weakening and destabilization of the target without compromising the physical integrity of one's own army.

[1] Sun Tzu, "The Art of War"

This multifaceted approach combines military and non-military actions. In the following points, we will focus on some of the most common approaches and add some additional key perspectives to understand current conflicts.

Cyberattacks: Their main types are sabotage of critical infrastructure, cyber espionage, Denial of Service (DoS/DDoS) attacks, use of malware, and data manipulation. Through these methods, it is possible to block, alter, and steal data from the targeted enemy, as well as cause malfunction of their devices in order to disrupt the normal flow of life in the area.

Cyberdefense: Early detection and response, Cyber Threat Intelligence, training and education, and public-private collaboration are some of the ways to protect relevant systems and information, as well as the transmission of communications.

UAVs: The use of drones (the most common type of Unmanned Aerial Vehicle) in warfare has emerged as an alternative and complement, cheaper than many of the previously used technologies. In addition to their main features such as information gathering and terrain surveillance, they stand out for allowing remote control without involving physical personnel, thus limiting potential human casualties for the user. Following recent conflicts, their uses have further expanded as anti-missile countermeasures, guided attacks with light explosives, and even heightened coverage ranges, localization, and communication. These and other advantages have made them an essential tool in current conflicts.

Disinformation and psychological warfare: The massive spread of fake news, propaganda, and manipulated narratives through social networks, media, and other platforms. These tactics create confusion and distrust, potentially sabotaging operations or causing population polarization.

AI: From cyberattacks and drones to disinformation, Artificial Intelligence is present in most areas today. Its ability to generate confusing narratives, automate processes, select targets, create deepfakes, and quickly provide responses makes this technology the main actor behind many of the most successful attacks of the last decade.

I.2 Case Studies

- **Ukraine Conflict (2014–2025)**

- **Cyberattacks on critical infrastructure**: Over the years, different attackers have penetrated the critical infrastructure of both sides of the conflict. Some of the main malware used in this conflict are:

  WhisperGate, IsaacWiper, and NotPetya[2] (the latter existing before the Ukraine war), often mistaken for ransomware which encrypts user data and demands a ransom, are in fact wipers[3]. Their main objective is to destroy data, causing irreparable damage to systems. They corrupt hard drive files and overwrite them with random data in such a way that, without backups, they become unrecoverable. Similarly, **HermeticWiper** was detected on the computers of Ukrainian organizations shortly before the Russian invasion of Ukraine.[4]

  - **KillDisk**, a destructive malware designed to damage and delete operating system files. It deletes system files to prevent the operating system from booting, even going so far as to encrypt files. It affects Windows and Linux systems, mainly targeting critical infrastructure and the financial sector in Ukraine.[5]
  - **Industroyer** and **Industroyer2**: This sophisticated malware was designed to disrupt Ukrainian critical infrastructure and was responsible for a blackout in Kyiv in 2016. Linked to Russian intelligence (GRU), this malware communicates directly with industrial

[2] Proofpoint, "Threat Reference: Petya," https://www.proofpoint.com/es/threat-reference/petya
[3] WatchGuard, "WhisperGate Ransomware," https://www.watchguard.com/es/wgrd-ransomware/whispergate.
[4] Recorded Future, "IsaacWiper continues trend of wiper attacks against Ukraine," https://www.recordedfuture.com/blog/isaacwiper-continues-trendwiper-attacks-against-ukraine.
[5] CCN-CERT, "Descubierta una variante del malware KillDisk que cifra sistemas Linux," https://www.ccn-cert.cni.es/es/component/content/article/4192-descubierta-una-variante-del-malware-killdisk-que-cifra-sistemas-linux.html?catid=23&Itemid=11827.

protocols and attacks and controls SCADA control systems[6].

AcidRain and **AcidPour**: The first of these is, once again, a wiper, but in this case it targeted the Viasat (KA-SAT) satellite network in Ukraine in February 2022. In this way, Russian intelligence, through another wiper, was able to interrupt enemy communications. On the other hand, AcidPour was the improved variant of AcidRain, but specifically designed to attack Linux x86 systems. Additionally, it is capable of overwriting itself in order to evade device defenses.[7]

Disinformation bot networks: Over the years, Russia has used various means to spread disinformation and fake news against Ukraine. Disinformation is currently spread mainly through social networks and news channels aligned with one side. One example of mass disinformation shared by pro-Russian accounts occurred in April 2022, blaming Ukraine for the massacre of more than 400 civilians in Bucha[8].

Operation Spider's Web (June 2025): Ukraine carried out a coordinated attack using 117 FPV drones self-guided by AI against five Russian airfields, from Siberia to Russia's western border. The drones, transported in trucks with remotely operated roofs, damaged or destroyed at least 12 aircraft, including Tu-95 and Tu-22M3 nuclear-capable bombers, causing estimated losses of 7 billion dollars.

- **Israel–Hamas Conflict (2023–2025)**

[6] ESET Welivesecurity, "Industroyer: amenaza cibernética derribó red eléctrica," https://www.welivesecurity.com/la-es/2022/06/13/industroyer-amenaza-cibernetica-derribo-red-electrica/. CISA, "ICS-Alert (IR-ALERT-H-16-056-01)," https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
[7] SentinelOne Labs, "AcidPour: New embedded wiper variant of AcidRain appears in Ukraine," https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/.
[8] EBSCO Research Starters, "Bucha Massacre," https://www.ebsco.com/research-starters/military-history-and-science/bucha-massacre.

- **Cyberattacks by Hamas on media buildings (October 7 and 9, 2023)**: On October 7, Hamas carried out a massive and unexpected attack against the State of Israel, launching thousands of missiles and capturing civilians. To support this attack, criminal groups such as AnonGhost carried out DDoS attacks against multiple websites. A DoS or DDoS is a Denial-of-Service attack,[9] meaning the disruption of a server or network by flooding it with abnormally high volumes of traffic, thereby overloading resources and causing a crash.

On October 9, 2023, the same hacker group exploited an exploit (a piece of code used to take advantage of a system vulnerability) in the RedAlert application,which sends alert messages in case of rocket or mortar fire, sending Israeli citizens a false nuclear attack alert[10].

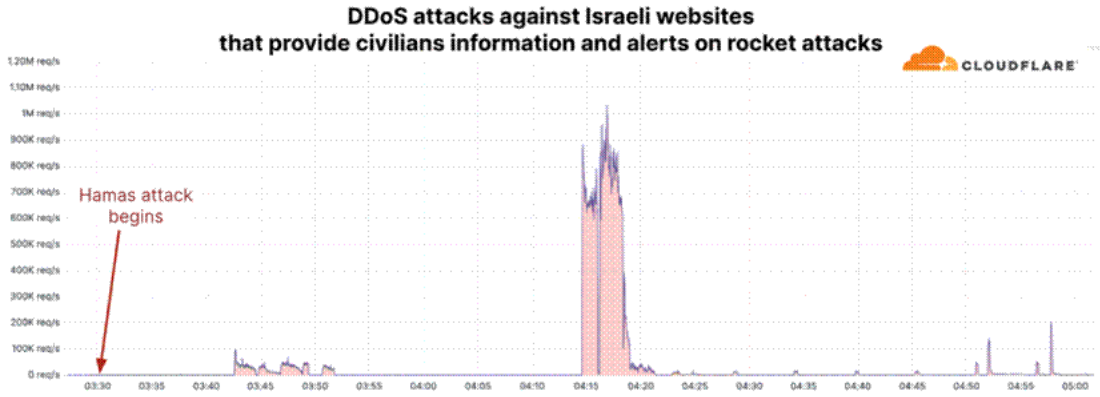


Figure 1.1: DDos Attacks Against Israeli Websites, Cloudflare 2023

- **Other conflicts**
  - **Libya (2011 onwards):** During the civil war in Libya, social networks, especially Facebook, were used to spread videos and fake news in favor of different sides. Among these

[9] Cloudflare, "Cyber attacks in the Israel-Hamas war," https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/.
[10] U.S. Embassy in Israel, "Emergency Preparedness," https://il.usembassy.gov/u-s-citizen-services/local-resources-of-u-s-citizens/emergency-preparedness/.

videos are supposed surrenders or false agreements between factions, aiming to proclaim fictitious victories. [11]

- **Electoral disinformation campaigns:** Around the world, cases of disinformation have been seen following presidential elections in several countries, such as in Brazil in 2022 and Guatemala in 2023. In Brazil, supporters of then-president Jair Bolsonaro shared false claims about fraud in electronic voting machines, which ended in riots. In Guatemala, false narratives were published aiming to influence public perception. [12]

- **Exchange of attacks between Israel and Iran (June 2025):** Under the pretext of destroying Iran's nuclear program, Israel launched attacks on Iranian soil. In response, Iran launched hundreds of drones and ballistic missiles. During the conflict, Israel employed hybrid warfare tactics such as selective drone attacks, sabotage, and infiltration by Mossad. Additionally, both sides have attempted to psychologically destabilize each other by using propaganda and disinformation, employing these methods to try to gain social support from other countries. [13]

[11] Swissinfo, "Guerra de noticias falsas para acompañar los combates en Libia," https://www.swissinfo.ch/spa/guerra-de-noticias-falsas-para-acompa%C3%B1ar-los-combates-en-libia/44907464.
[12] Pensamiento Iberoamericano, "Narrativas de desinformación en América Latina: patrones y operaciones de influencia en el ecosistema digital," https://pensamientoiberoamericano.org/1-2024/narrativas-de-desinformacion-en-america-latina-patrones-y-operaciones-de-influencia-en-el-ecosistema-digital.
[13] Harvard DRCLAS, "Battle Against Fake News: Brazil's 2022 Elections," https://www.drclas.harvard.edu/event/battle-against-fake-news-brazil%E2%80%99s-2022-elections.

II) Economics of Cyber Warfare

II.1 A Break of supply chain

A) Wealth transfer, hijacking the Banking system

Cyber extortions or malicious data breaches have heavily affected the financial sector, with extreme losses reaching $2.5 billion.[14] Such severe incidents of cyber attacks on major financial institutions could position macrofinancial stability in grave danger, with the effects including the disintegration of: confidence, critical services, and technological interconnectedness. To emphasize the intensity of hijacks of the banking system, negative impacts on profitability are felt for the 12 quarters (3 years) following a breach.[15] These circumstances align with the idiosyncratic viral loss theory, instead of traditional macroeconomic theory since an unexpected event, cyberattacks in this case, lead to sustained losses. Therefore, an immense strain is imposed on firms because they are unable to adjust quickly for profitability maintenance. Large and privately-owned banks tend to feel the negative consequences more significantly, as they experience decreased loans and deposits, alongside an increase in liquidity to take care of unpredicted expenses. Furthermore, damage to technological assets and service disruptions cause data breaches and cyberattacks which then lead to overwhelming operating costs.[16]

There is a thin line that distinguishes criminal activities from state-directed operations, and in modern times, this line becomes more blurry by the day. A prime example of this is Lazarus – a hacker group allegedly linked to the government – which brings together conventional espionage and comprehensive economic corruption. Numerous operations spanning over the last decade – including the Sony pictures breach and the Wannacry global ransomware attack – have been executed to raise capital for the Democratic People's Republic of North Korea (DPRK) regime. The aim being to avoid sanctions and to invest in black-market programs.[17] Consequently, the threat landscape is more widespread

[14] IMF, *Global Financial Stability Report*, April 2024, Chapter 3: "Cyber Risk: A Growing Concern for Macrofinancial Stability."
[15] *ResearchGate*, "An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States," (2023).
[16] *ResearchGate*, "Idiosyncratic Viral Loss Theory: Systemic Operational Losses in Banks," (2021).
[17]

and complex as the existing convergence between state-orchestrated activities and privately-owned group transactions complicates defense strategies and blockages.

Data blockades and trade impairments lead to substantial and interconnected economic fallouts. Financial damage, destruction of imperative information, and interference of valuable infrastructure are all significant consequences of cyber attacks. Such effects play a huge role in economic losses, with the average data breach cost being $4.88 million worldwide. [18]

B) The New Version of Naval and Land Blockade

The digitization of open trade became the 21st century's big step towards globalization of production. This would magnify the effect of cyberattacks within the supply chain of goods. Let us go back in history, and witness the main purposes of naval and land blockade.

Back in the Napoleonic war, the British Royal Navy implemented a continental blockade, which was draining most of their military resources as the big operation required extreme labor force, constant awareness, and excessive raids. However within the 21st century, cyberattacks became the easy way in by breaking rationality. Bringing in the same scenario within the Russo-Ukrainian war, we can witness how cheap such a blockade became within the wheat farming industry. Ukrainian land recorded an overall amount of 7.4 million USD worth of attacks of ransomware and malware during 2022. [19]

However, the most notable impact is the Russian blockade of Ukraine within the outside world. On the first day of the invasion, 24th of February 2022, Russian intelligence interfered with the Viasat satellite, and disrupted Ukrainian internet connection, causing them to lose contact with the outside world. This splurged within miscoordination where reaching out to new harbors was impossible.[20] Due to weak global demand, the wheat prices rose, while Ukraine decreased its production of this primary commodity by 27%.[21]

---

[18] IBM Security, *Cost of a Data Breach Report 2024*.
[19] SentinelOne, "AcidRain: A New NotPetya-like Wiper Targeting Ukraine," (2022).
[20] *Ibid*
[21] IFPRI, "Ukraine and global agricultural markets two years later," (2024/2025).

C) The open market, blockade of natural dependencies

David Ricardo's trade theory confirmed the idea of "everyone benefiting from trade". However, this pattern would be witnessed in two nations with no risk of war anyhow. With the rise of the global open market, each country decided to specialize within their own specialty, creating regions based on output. This specific good that can be produced effortlessly by one land would work as a medium to acquire other commodities. [22]

While this allowed the world to produce faster, quicker, and at a better quality, the hybrid conflicts would cause an easy blockade of a certain commodity; calling in the disruption of the supply chain. While the Ukrainian example can be portrayed by the rise in the price of wheat[23], the nation of Taiwan leads a massive risk within the supply of semiconductors.

Witnessing the supply chain of the world, hybrid war influence spurges within the security of various elements. Let us take into consideration the aforementioned supply chain, where to secure the production of a certain good depends on multiple interconnected tasks. The O-Ring theory suggests that the probability of achieving production relies on the completion of each task. With the rise of the open market each location has used their comparative advantage in order to maximize expectations.[24] Let's take the example of a phone: its semi-conductor fabricated in Taiwan, constructed in China, based on a model designed in Silicon Valley, with a code developed in India and the US, shipped by a French company, and sold in a Swedish Franchise. If any player fails to do its task, then the whole phone would deteriorate.

Each one possess a certain probability of achievement, which makes the outcome close to one if we are actually using the comparative advantage

[22] Ricardo, D. (1817), *On the Principles of Political Economy and Taxation*.
[23] *Small Wars Journal*, "Putting Operation Spider's Web in Context: Remote Drone Attacks on Russian Airbases," (August 2025).
[24] Kremer, M. (1993), "The O-Ring Theory of Economic Development," *The Quarterly Journal of Economics*.

However,$\Pi p^i \approx 1$ as we are having a multiplication series in that case, if only one component fails to do its job, the whole outcome drops to 0, making production nearly impossible, as the current world is not ready for such types of shocks.

II.2) Discouragement of Investment

While it is no secret that war discourages investment massively within a nation, this part delves deep into the economic theory of hybrid warfare. Investment is not only based on how much capital is present and active nowadays, nor the interest rate alone. Instead, it depends on a mix of variables where hybrid warfare does play a role within risk aversion and probability of failure. The "Guns and butter" contrast offered deep insights into how the Hybrid War is reshaping investment trends nowadays, leading to various neglect of the butter sector. Heavy militarization brings us back to the massive dilemma of development. While it does benefit humanity by increasing efficiency, it also magnifies violence, and the rule of the wolf over the sheep.

A) **Reverse Romer: Miscoordination amidst conflict**

A major explanation of the rising inequalities between nations can be explained within Romer's interpretation. As the world nowadays gets globalized, people have a choice on 'where' to invest, not only how much. This extra benefit arises after witnessing the benefits of trade, making the whole globe a huge economy. [25]

However, it marked one big critique of globalization, where the rich nations were getting richer, and the poor were getting poorer. Romer explained the economic phenomenon by his first claim of 'endogenous technology'. We already know that technology is a factor of production and complements capital (the result of investment). Moreover, technological advancement in a certain country makes the return of investment more

[25] Romer, P. M. (1990), "Endogenous Technological Change," *Journal of Political Economy*.

beneficial, as it increases the productivity of future capital. Within that scheme, Romer suggests that Technology is defined by a certain level of investment, it does not come out of nowhere A(K). In order to explain the rise of places like Silicon valley, he claimed that our choices of investment are rather based on the expectations of other people's investment, causing either a miracle or a blessing. Since coordination is key towards economic growth, there must be great expectations of others in a certain region to keep up the economic blessing.

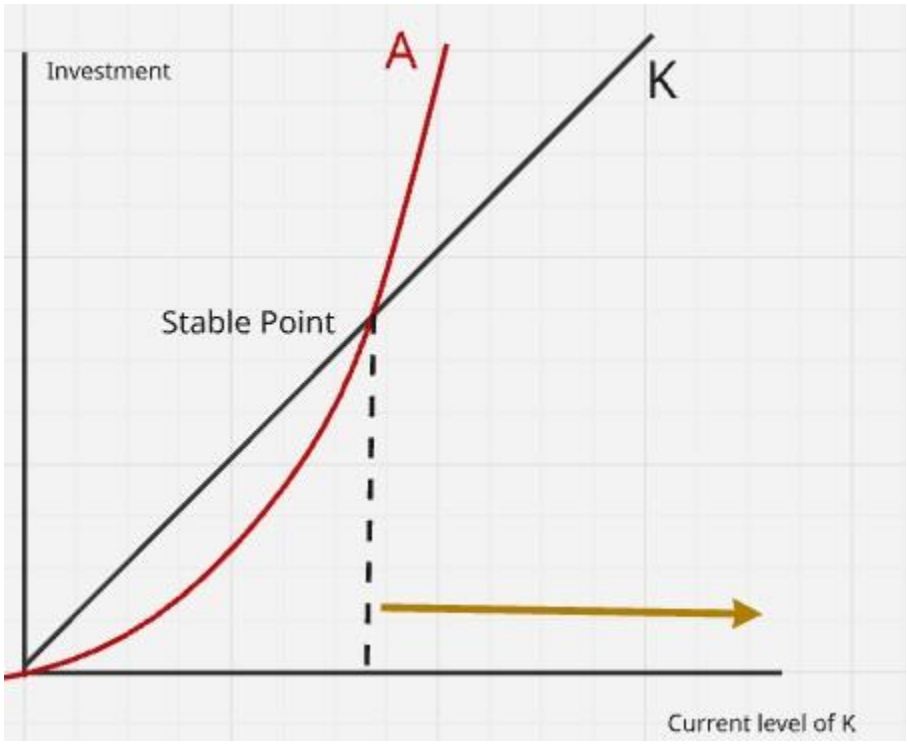


Figure 2.1: A Romer Model Example with the Endogeneity of Technology

The Romer model would look like the above graph, where A symbolizes the level of investment into technology, and the K line is the 45 degree line which elaborates on the expectations of other industries' investment. However, let us not forget that each one of the companies is thinking individually, but the aggregate outcome is hardly ever meeting the expectations. If we are on the golden arrow, we can witness that it would be more beneficial for companies to invest more than the expectations of others. This causes people to raise their expectations in the following period, and thus keep on investing more and more. The other side of the stable point seems like the dystopian scenario of investment, where it would

be more beneficial to invest less than the expected level. This causes a decrease in expectation in the next period, until converging towards a 0 investment level. Thus, the situation of being in either a 'blessing' or a 'curse' is fully based on expectations, which makes various top notch nations vulnerable nowadays.

As we have seen, coordination is paramount to sustain a high economic growth, explaining the Korean miracle and the rise of China as a superpower. However, let us witness within the lens of a cyberthreat in the middle of a hybrid war and see what would happen in that case. We can take into account that investors do not know each other's type. Some would not care that much, while others would rather be risk averse, causing them not to invest anyhow in the presence of a certain cyberthreat that may damage their machinery. While identifying the type of all the investors is difficult, various firms would start to shift their perspective towards investing less. This is due to the rather common-sense idea that some firms would not invest in a technology where risk can take over, which might lead from a blessing pathway to a sudden cursed one. This can be illustrated through various examples of victim countries.

Prime examples of tools for innovation and sustainability are reversed into weapons of human destruction which include, yet are not limited to, Ukraine and Estonia.

Profound distress, widespread destruction, and countless losses in just 3 years. The lengths of devastation that haven't existed since the second World War. The war in Ukraine has led to 42,000 civilian casualties, the crippling demolition of 3,600 educational institutions,[26] and 12.7 million people in need of aid.[27] Due to the dire consequences of war, the nation's focus is forced into survival mode. – Additionally, due to the complete divergence of resources and attention towards military defense, it neglected the conditions required for endogenous economic growth.

Asynchronization is particularly noticed in Ukraine's incremental acquisition – one system at a time – approach; creating drastic time gaps between the supply of advanced systems and their actual launch onto the battlefield. For instance, British

[26] ReliefWeb, "Ukraine Emergency: Three Years On - 2025 Update," (February 2025)

[27] UN OCHA, "Ukraine Humanitarian Needs and Response Plan 2025," (January 2025).
UN OCHA, "Ukraine: Summary of the Humanitarian Needs and Response Plan," (January 2025).

Storm Shadow missiles weren't used in actual combat until May 2023, and the same situation applies for U.S. Army Tactical Missile Systems which were only provided in October 2023. Ultimately, a capability gap is created as there's a mismatch in pacing since Ukraine's military requirements are determined by Russia's high speed attacks. A[28]s a result, economic and social costs drastically increase as a result of miscoordination between Ukraine's needs and the response from its allies – with them also considering their most suitable, individual political interests. In terms of regional stability and democratic principles, the stakes for some allies are not existentially threatening in the same way. The varying degrees of urgency, cost sustenance, and prolonged strategic determination are caused by the inherent imbalance that exists in how stakes are perceived. Conclusively, there's a collective action issue shown in the delays of military assistance – incremental acquisition consequences– further complicating the process of obtaining unity, and decisiveness in strategy, eventually leading to miscoordination.

Due to the collapse of productive capabilities and territorial occupation, current output is close to potential, according to the National Bank of Ukraine. Alongside the challenge of declining economic and military aid, specifically from the US, 50%[29] of its electricity power generation has been destroyed – reducing productive capacity. It is experiencing extreme fiscal deficits, as well as growing trade deficits. Foreign aid has existed as a major pillar in maintaining social welfare, and the risk of losing it could potentially lead to an absolute economic destabilization[30]. Therefore, a vicious cycle exists where military miscoordination leads to economic miscoordination, which creates military weaknesses. This is a clear reflection of the "reverse Romer" effect, in which the nation's economic engine is systematically dismantled due to a chain of interlinked military and economic breakdowns.

Stemming from the globalized world that we live in today, a domino effect between nations is created. When one nation makes a singular movement, a chain reaction is triggered across the world that no border can withstand. A prime example of this – amongst other nations – is the alliance between Ukraine and Estonia in this war. Although Estonia is not experiencing the direct "reverse Romer" effects of conflict, it still acts as a key player throughout the great collapse and turmoil, and therefore carries the consequences of existing as such. Miscoordination could be witnessed both in its "unwavering support" for Ukraine,

---

[28] UN OCHA, "Ukraine Humanitarian Needs and Response Plan 2025," (January 2025).
[29] World Bank / Government of Ukraine, *Rapid Damage and Needs Assessment (RDNA3)*, (2024).
[30] UN OCHA, "Ukraine Humanitarian Needs and Response Plan 2025," (January 2025).

as well as its participation as a North Atlantic Treaty Organization (NATO) and European Union (EU) member. However, in contrast to Ukraine's initial struggles with discoordinated aid, Estonia's ongoing engagement with NATO exemplifies a forward-thinking approach aimed at avoiding "reverse Romer" dynamics. This is highlighted through Estonia and its allies' efforts in building a resilient coordination system to deter external threats from Russia. Acting as not only a tactical necessity, but also a long-term investment in committing to national security, stability, and growth.

B) Dutch disease: Even the attacker is at risk

As Shakespear muses: "A Jack of all trades is a master of none, but oftentimes better than a master of one." This dramaturgical quote has long been used in economics to encourage the claim of diversity within the economy. The so-called Dutch Disease, where a country decides to ultra-focus on one specific sector while neglecting the others has majorly affected various nations into economic vulnerability. [31]

However, what does it have to do with Hybrid warfare? As previously claimed technology is endogenous, and the result depends on how much investment has been spent on it. One major player in this game would be the government. They can allocate their spending to one technology more than the other, leading to its specialization. However, the Dutch disease manifests itself. To simplify the economic phenomenon of the disease in case of hybrid war, we will split the economy into 2 major sectors

1) The consumer sector (Butter)
2) The military sector (Guns) [32]

The nation's GDP would have the formula of $Y = A_B * K_B^{\alpha} * L_B^{(1-\alpha)} + A_G * K_G^{\beta} * L_G^{(1-\beta)}$

[31] Corden, W. M., & Neary, J. P. (1982). "Booming Sector and De-Industrialisation in a Small Open Economy." *The Economic Journal.*
[32] Stockholm International Peace Research Institute (SIPRI), "Guns And Butter"

The subsymbol of "B" stands for Butter, and "G" stands for Guns. The derivation would portray a complementarity between the components of the same sector, and substitution if another sector increases.

The Blue collar labor market can be manifested as a market where individuals shift from one sector to another easily based on higher wages, until achieving full parity. We can derive the labor demand function based on "The marginal product of labor" and every firm would assign a wage (w)= MPL in order to maximize their profits.

$$MPL_B = dY/dL_b = (1 - \alpha)A_B * (K_B/L_B)^{\alpha}$$

$$MPL_G = dY/dL_G = (1 - \beta)A_G * (K_G/L_G)^{\beta}$$

The wage in each sector would be defined by the equilibrium between the Labor supply and Labor demand. It is worth mentioning that wages must be equal in both sectors as we are talking about the Blue collar sector. If one wage is higher than the other, laborers would shift sectors, increasing the supply in one sector at the cost of the other.

Figure 2.2: Theoretical Real wage equilibrium between the two sectors

As the graphical representation shows, the wage must remain the same. However, as hybrid warfare is on the rise, the increase in government spending in the military sector, would lead to a rise in A(G) thus increasing Labor demand in this sector, which would increase the wages temporarily, as the shift for butter to guns would reset the wage rate into parity.

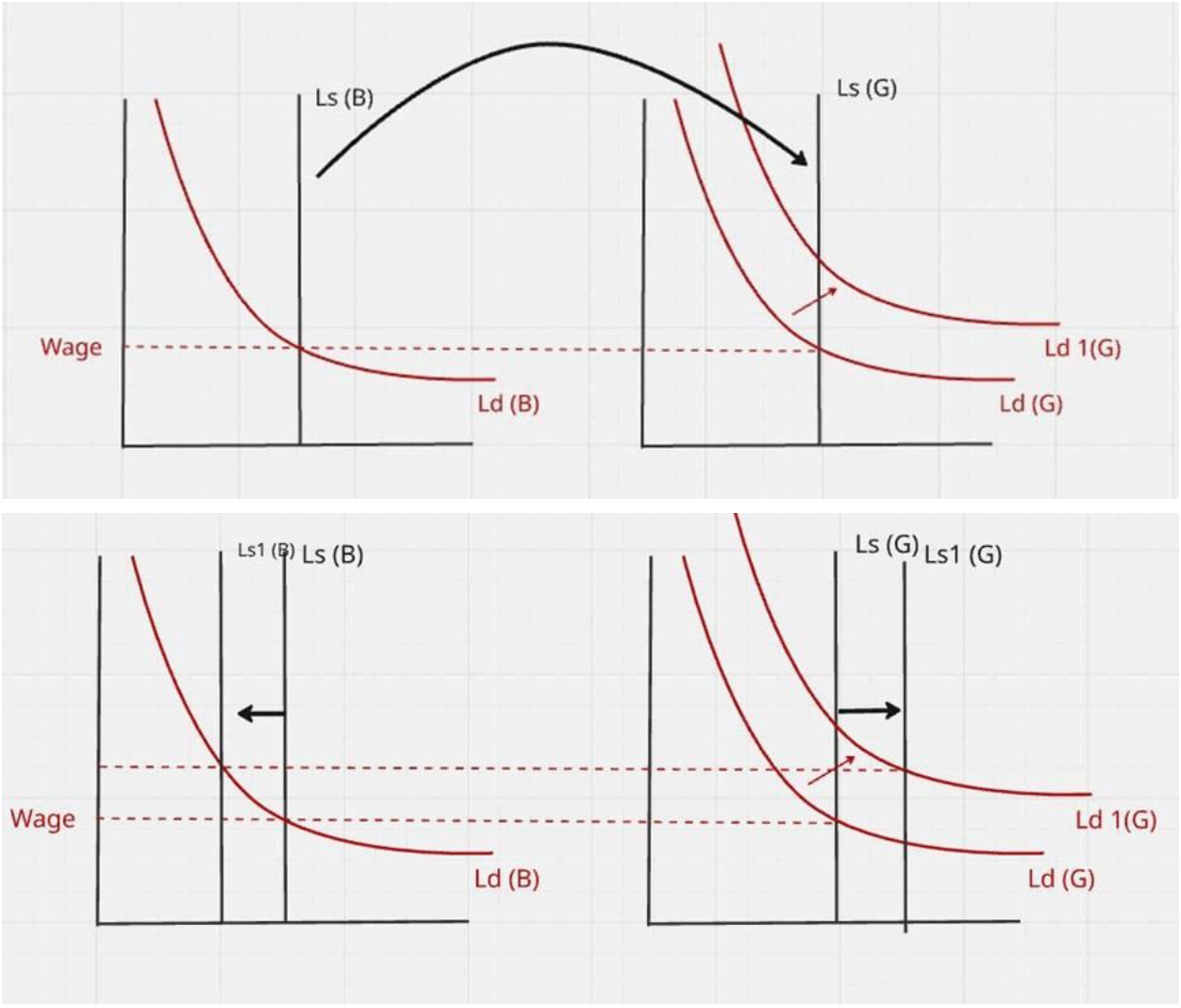


Figure 2.3: The Change of the labor supply following a shock in a certain sector.

This focus into one technology into another, will lead to the Guns sector developing and the nations specializing in it specifically. It would not take long as well until machines get rented into the military sector, which is due to higher return and higher rental rate, thus continuing this loophole of butter shrinkage.

We can witness this example within the Russian federation after declaring war on Ukraine. Its government spending increased by 1 trillion rubles[33], being taken from the consumer economy. This had major consequences on the butter sector of the nation; causing various sub sectors to collapse, with retail spending shrinking by 9.3% by 2022, and the automotive industry going down by 59%. [34]

C) Capital depreciation: Insecurity and expectation (28th)

Looking at it from a business viewpoint, capital depreciation can be defined as assets' – workstations or industrial machinery – value diminishing over time. This can be caused by a number of factors, including obsoletion of technology, fluctuation in demand for an item, and high reparation costs. Now, a strategic tactic to reach geopolitical goals is the intentional use of economic pressure, which acts as a critical dimension of hybrid warfare. A key example of this is the explicit combination of military, economic, diplomatic, and information means of China's hybrid warfare strategy on Taiwan, which notably increases the latter's weakness. There exists a deliberate effort to deteriorate a nation's economic stance through intangible means, through the systemic exploitation of its economic factors. The curated result of non-kinetic actions, that aims at destructing an economic basis, expectedly leads to the depreciation of capital. As a result, economic risk is fundamentally shifted from market forces to strategically driven measures of hostility. Furthermore, national GDP, trade, energy markets, and financial stability end up being at stake.

In an era of hybrid warfare, a nation's industrial policy and independence in defense production are significant economic resilience factors. A case that exhibits this is that of Greece and Turkey. It reveals divergent outcomes since they have different strategic economic structures. Thanks to its robust domestic defense industrial basis (DIB), Turkey experienced a positive correlation between an increase in defense spending and GDP growth. Consequently, it can be assumed that a response to hybrid threats, which localized domestic production, can stimulate endogenous economic growth. The opposite of these circumstances is shown through Greece, with the nation being incredibly dependent on imported defense equipment, thus experiencing a negative correlation. This is because

[33] CEPA, "Stormy Weather Pummels Russia's Economy," (May 2025).
[34] KPMG International, "The impact of the Russia-Ukraine war on the auto industry," (2023).

defense spending has diverted valuable resources from other sectors of production. Whereas Turkey's approach contributed to a better use of limited public funds, developing a more skilled working population, and attracting foreign direct investment (FDI). Conclusively, a nation's economic foundation – production sectors – greatly influences its security and how it can deal with future threats.

Economic instability develops an important challenge to nation–wide infrastructure investment planning. Budget deficits and federal funding cuts often force governments to make difficult trade-offs on how to prioritize spending, including in areas like infrastructure and technology. Investment in technology and infrastructure is often perceived as "invisible," making it difficult to secure adequate funding from policymakers who may question the tangible returns on such investments, due to the unpredictable nature of capital allocation. Regardless, investment in protection for critical infrastructure is more vital now than ever before, and is becoming more so with the increased climate risks and political shakiness we are witnessing worldwide.[35] The climate crisis makes infrastructure systems face escalating hazards, leading to immense uninsured losses. For example, in 2024, environmental catastrophes added up to $386 USD billion in losses, with only 40% insurance coverage. This calls for a sustainable restructuring of how private firms are intertwined as support systems for public goods. Acting proactively is now a crucial factor in asset valuation, and the sustainability of a nation's capital. [36]

D) Guns and Butter: Shrinkage of the private sector

The Guns and Butter analysis has been developed in Stockholm to deduce the shrinkage of the private sector due to ongoing change in opportunity cost. This is derived from what we call 'the hollow out effect', a major disadvantage of government spending.

The hollow out effect suggests that Public investment (government spending) would take space in the economy, leaving the private investment demotivated and regressed. In this analysis, we are going to start by defining the Guns and Butter, then portraying the indirect effect of Hybrid war, on both the attacker and the victim. Let us divide the economy into two major sectors, the Guns sector (military) and the Butter sector (civilian). In any case of war, the

[35] ISOEC, "Between Turkish Defense Industry and Economic Growth Analysis of Relationships," (September 2025).
[36] Munich Re, "Climate change presses on: Devastating wildfires and intense thunderstorms exacerbate losses," (January 2026).

population is going to be conscripted due to higher wages and overall needed conscription. However, the effect of hybrid warfare development would lead to a massive shift off situation. We can already witness in the news a massive rise in the military sector, creating new bureaus, and increasing budget.

The Solow model would help us derive the overall economic induction behind the results that we are witnessing today. Taking the general sense of investment, we can assume that Guns and Butter are substitutes, or in other words, the growth of one would be at the expense of the other. The Solow model explains a rather optimistic approach to reveal the end game true value of capital or investment present in a certain sector per capita.

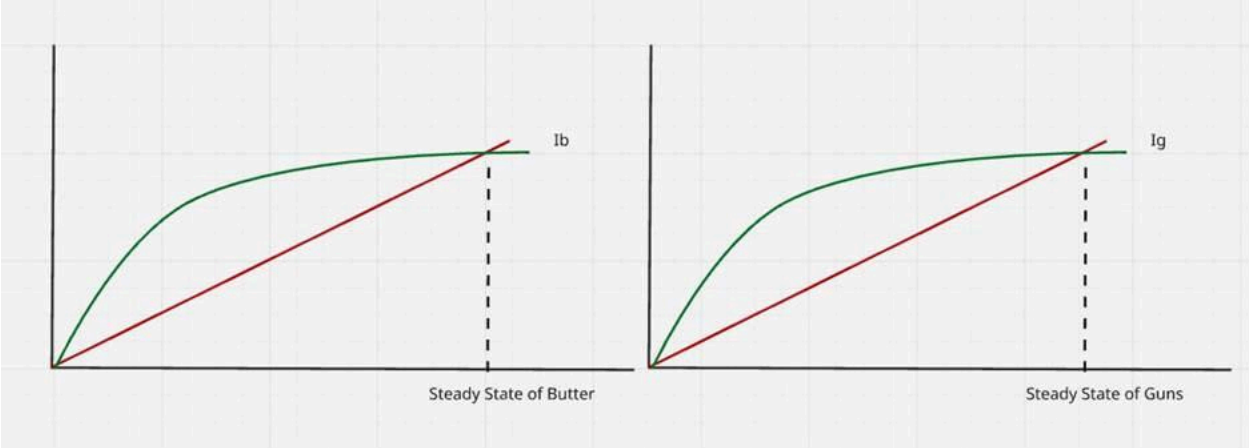
$\widehat{y} = \widehat{k}^{\alpha} * \widehat{h}^{b}$ where y symbolizes GDP per capita, k capital per capita, and h human capital per capita. Now we would use this Solow identification with two sectors, exploring the dynamics between the two. The investment per efficient worker would be based on the saving rate which is in that case

$$\widehat{i_G} = s_G * \widehat{k_G}^{\alpha} * \widehat{h_G}^{\beta}$$

$$\widehat{i_B} = s_B * \widehat{k_B}^{\alpha} * \widehat{h_B}^{\beta}$$

Where G symbolizes the Guns sector and B for the butter sector. The total depreciation would be based on a certain depreciation for each sector. We can safely assume its representation would be linear.

Based on a certain depreciation rate for each sector, we can safely assume that its representation would be linear.



Assuming originally a steady state, the effect of Hybrid war would lead to a shrinkage. The economy converges into a certain point, based on past and current new variables. The introduction of hybrid war could be manifested as an increase in technology in the attacker's economy. While it may not be valid in the "Per efficient worker analysis", it called for higher wages in this sector as the Dutch disease explained above has proven. Thus, the high human capital workers would rather prefer to lean more into the guns sector. This causes the h variable to decrease, and in the butter sector and increase in the guns sector. As the Guns sector is taking more of the upper threshold of human capital.

A re-evaluation of the typical "Guns and Butter" model is manifested with Israel's distinct economic and geopolitical context. Because the nation has a unique position amongst large-scale industrial sectors, greatly defined by ongoing and fundamental challenges to its control, it requires sustainable and consistent investment in national defense. It is important to note that Israel has experienced a significant economic transformation, despite everlasting security necessities. This is highlighted in its evolution from an economy that has historically relied on secured agriculture and manufacturing, into one that is internationally renowned as an agenda-shaping catalyst in innovative, high-tech industries.[37] A well-structured defense system is perceived as the foundation for Israel's economic stability, as it does exist as a nation that has been operating against profound contestation to its authority – since its formation in 1948. The factors required for endogenous

[37] Bloomberg/Israel Ministry of Foreign Affairs (2026) "Israel's high-tech sector breaks records despite wartime challenges."
Startup Nation Central (2025). "Abraham Accords: Tech Investments Redefining Cross-Border Collaboration."

activity, Research and Development (R&D), and investment are absolutely defined by Israel's level of security. Therefore, defense spending isn't merely a cost for the nation, but a fundamental building block to ensure its survivability.[38] All while keeping in mind that it is a state that has been built on the suffering of the indigenous people of Palestine who continue to resist the occupation and advocate for their own independent state. Consequently, the opportunity cost of military investment isn't simply diminishing social welfare or the growth of the private sector, but rather the value surrendered of the choice not pursued of insufficient military spending, which could completely destabilize the economy. As a result, a rare economic interdependence is created as "Guns" are desperately needed for the "Butter" sectors to flourish.

Because Israel continues to sustain an unrestricted position towards foreign capital, and incentivizes Foreign Direct Investment (FDI) through grants, low tax rates, and tax exemptions, companies and governments are conducive to invest, which offers immense support for upholding its economy. A secure investment environment is ensured by the legal system's structure – safeguarding the rights of international and domestic entities in their establishment and creation of businesses, while also maintaining equal competition. Furthermore, the investment landscape is finetuned thanks to Israel's government's policy goal of transparency of its regulatory system, which involves actively reporting publicly and public participation. Moreover, Israel's commitment to transparency is highlighted by its participation as a member of the UN Trade and Development (UNCTAD) organization's global network that vouches for unconcealed investment procedures.

However, regardless of these efforts, competition is still inhibited by the overwhelming presence of monopolies and oligopolies in several industries, including marketing, agriculture, and communications infrastructure. Accordingly, this can lead to limiting the full potential of private sector growth and reduce the purchasing power of Israeli citizens. To add to that, there is a growing budget deficit due to the fiscal liability of widened defense spending. Not only that, measures such as increases in value-added tax (VAT), domestic insurance contributions, and a reduction in paid recuperation days are included in the 2025 budget proposition, which could lead to a decrease in aggregate demand (AD) levels. [39]

---

[38] **NBER Working Paper.** "High Tech and Venture Capital Inflows: The case of Israel."

[39] Carnegie Endowment for International Peace, "The Abraham Accords After Gaza: A Change of Context," (April 2025).

Stimulating a competitive, transparent, and booming private sector ("Butter") in Israel becomes increasingly difficult with the intense maintenance required for its robust defense system ("Guns") to sustain its economic stability. This leaves the government with a complex cycle where escalating constraints are faced in balancing the financial well-being of its citizens ("Butter") with its national security ("Guns"). Although there are existent policies to actively encourage FDI and R&D, the persistence of local monopolies and fiscal pressures, which are imposed by defense spending, lead to endogenous economic obstacles. Through the naked eye, any person may see Israel's economic management as successful trade-offs between the Butter and Guns sectors of the nation. Yet, when observing Israel's unique economic model through a microscopic lens, a critical question is raised: how sustainable is the economy independently, without sustained foreign investment – particularly from its Western allies? To put it simply, without the consistent investment and political support from Western partners, such as the United States of America and Germany, to name a few, the equilibrium between military spending and economic vitality may not be maintained to the extent that it is now. [40]

```
. regress fdi cinc, robust

Linear regression                               Number of obs     =         63
                                                F(1, 61)          =     309.03
                                                Prob > F          =     0.0000
                                                R-squared         =     0.3676
                                                Root MSE          =     28.263

------------------------------------------------------------------------------
             |               Robust
         fdi |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
        cinc |   .0070095   .0003987    17.58   0.000     .0062121    .0078068
       _cons |   10.67142   3.595362     2.97   0.004      3.48205    17.86079
------------------------------------------------------------------------------
```

Since 2020, made possible by the signing of the Abraham Accords, relations between Israel, and several Arab nations – including the United Arab Emirates, Bahrain, and Morocco – represented a historical diplomatic achievement for some parties. Their shared strategic

[40] **NBER Working Paper.** "High Tech and Venture Capital Inflows: The case of Israel."

perspective of regional obstacles motivated these states[41] to open new trade opportunities, as well as operationalize access to advanced technologies.

Due to the continuing destruction of territory in Gaza, Arab-Israeli contact has been hindered, making interactions state-to-state and business transactions discrete. In spite of these constraints, adaptive economic responses have been carried out amidst geopolitical challenges. For example, Israeli companies possess the ability to bypass Red Sea shipping threats, driven by the emergence of a new land route between the UAE and Israel – across Saudi Arabia and Jordan. Notably, normalization between Israel and Saudi Arabia is beneficial on the latter's part because of Israel's high-tech advancements in artificial intelligence, biotechnology, and agricultural technologies. Layered onto this is Saudi Arabia's Vision 2030 development plan, with its megaprojects like NEOM, which would make Israel's potential contributions all the more vital for success.

On the other hand, broader regional conflicts, – such as the war on Gaza in Palestine and threats to maritime shipping by militant groups like the Houthis in the Red Sea – have had impactful effects on Israel's stability. With hostilities against Palestinians undermining multilateral regional strategies like the India-Middle East-Europe Economic Corridor (IMEC), and endangered critical trade routes requiring the search for alternatives – as well as supply chain diversification. Additionally, the Israel-Hamas upheaval has greatly affected Israel's export-oriented economy, as the current political situation has led to chaos in international economic frameworks and disruptions in the execution of global trade.

The culmination of these differing factors serve as indicators of the strategic distinctiveness of Israel's economic architecture. Although Israel faces persisting regional dilemmas, along with the consequences of geopolitical constraints, these issues serve as powerful influences of strategic economic adaptation. [42]This is highlighted by diversification of foreign investors through the pursuit of the Abraham Accords, accompanied by the mitigation of trade corridor blockages when confronted by threats in the Red Sea, both of which enhance Israel's long-term resilience. Residing in a volatile location, there is a clear interconnectedness between Israel's "Guns" (military security and mitigation of threats) and "Butter" (economic trade, FDI, and R&D). Because Israel's economic development tactics to complex transnational realities are direct and innovative,

[41] Carnegie Endowment for International Peace, "The Abraham Accords After Gaza: A Change of Context," (April 2025).
[42] Ibid

which stems from foreign support, its ability to avoid private sector shrinkage ("Butter") is heightened.

II.3) Technological regression

Hybrid warfare presents a paradox within technological advancement. Seeing the various dystopian movies like The Hunger Games, or even The Man in the High Castle, authoritarian regimes are usually portrayed with massive technology; however, it is not being used for consumer benefits, but rather for heavy militarization. This part portrays how hybrid warfare plays a role within constructing the dystopian societies that we are thrilled to watch. The Dutch disease presented above already portrays the hollow out of the consumer sector following the Guns technological advances. However, this part incorporates game theory, and highlights the inefficiencies that it might imply within production and economic growth. Thus, this specific technological advancement was born at the expense of a technological regression in the remaining sectors.

A) Drainage of technology and fear factoring

Controlling over 50% of the total semiconductor production, the small island of Taiwan is paramount for the technological progress of the modern world. Computers, cellphones, and many more gadgets rely on Taiwanese semiconductors. [43]

The Chinese (mainland) threat over the small island of Taiwan peaked at around 4300 cyber-attacks in a single day, mostly linked to organizations of cyber-espionage like Chimera and Stone Panda. Taking a closer look into this specific threat, a constant upgrade in cyber-security is causing an outflow increase in the average production of the microchips and raw material used in capital production. [44]

However, what does this imply to the general cost? We are talking about the raw material of the raw material. In a digitized world, factors of production revolve

[43] **Jetir.Org (2025).** "Microchips and Macroeconomics: The Economic Impact of Semiconductor Supply Chain."
[44] **Bloomberg Analysis (Welch et al.).** "The $10 Trillion Cost of War Over Taiwan."

around computers and telecom, which lead to massive dependency on microchip in any scale level. Cybersecurity spending in Taiwan has increased by an aggregate level of 100 million USD in the span of 2 years. This sponsors the claim of the rising Chinese threat. If one day the system collapsed, the entire world would face a semi-conductors shortage, leading to global technological regression, and a potential mismatch to future production.[45]

Let us bring back the idea of GDP based on factors of production

- Technology (A)
- Capital (K)
- Labor (L)

As Romer explained, technology is endogenous, and based on a certain level of capital and the nature of the capital itself. We cannot expect a correlation with technology if all our capital is mostly buildings instead of computers and machineries. Here we have it, a reduction in semiconductor production would eventually lead to lesser competition. The pattern of creative destruction and innovation would slow down. Therefore, humanity would not acquire the same amount of technology that it expected.

On top of that, the depreciation rate of capital would also lead to a certain fallback. With the rising threats of complete deterioration of our gadgets, and most importantly, the exponential doubling of malicious files on the web; computers and digital material that are connected to the web are facing a lifespan decrease, with an expected timeframe of use constantly increasing.

On both sides, this new trend of hybrid-war is damaging our technological progress; from depreciating our current level to discouraging an increasing technological advancements, hybrid conflicts are the nuclear bomb of the cyberworld.

B) Adaptability of new technologies and their vulnerability

As the digital revolution of the 21st century made every data gathering within hardware, hybrid war led to the emergence of various new sectors,

[45] *Ibid*

including the 'cyber-security'. Looking back at the different cyber-attacks, we cannot deny the rise of cyber-security precautions within it. This brings back the guns and butter dilemma.

However, as nothing is free in this world, the rise of hybrid warfare would potentially lead to an increasing budget within encryption systems, whether from the private or public sector. This nonetheless would actually lead to a potential increasing trade-off between Guns and Butter. As we are including an extra cost within the militarization of a certain nation, it must as well lead to larger price within producing military weapons, only to fall to a new cybertrap.

The curse of evolution, has led to a higher trade off and shrinkage of the production possibility frontier of certain countries. We can consider it as an irrational choice to produce weapons under 'obsolete' technology as they are becoming more and more likely to be cyber-attacked and totally depreciated; leading to a cost of rational guns to a high rate compared to past ones.

The concept of creative destruction has been developed by Josef Schumpeter as an explanation of innovation. People usually innovate to erase a certain competitor who did not acquire this specific creativity. However, this theory was supposed to be positive within the scheme of macro-economics, causing progress of society. However, the science gone wrong really shifted the tables upside down. [46]

Applying the scheme of creative destruction within an actual destructive scenario, the chain would go as follow:

Phase 1: The creation of new hybrid warfare weapons, This would be characterized as a major start of the chain, as we can take the example of the Wannacry virus: A major virus that drained a lot of bitcoin wallets with a ransom in exchange.

Phase 2: Anti malware development: This led to a lot of countries, majorly the UK to respond with an increasing demand of cybersecurity to finally neutralize the virus. [47]

[46] Joseph A. Schumpeter, *Capitalism, Socialism and Democracy* (New York: Harper & Brothers, 1942), 81-86.
[47] **MDPI (2025).** "Destructive Creation of New Invasive Technologies: Generative AI Behavior."

Phase 3: Malware development: The development of the new weapons acquired by British technology led to a more sophisticated warfare, and thus a higher cost of weapons due to higher risk of getting damaged. However, hackers would not give off so quickly leading to the creative destruction of this new cybersecurity example, just like the Solar Wind Hack, which remains unsolved till nowadays, which would seem as if we returned to the 1st phase. [48]

As we can see the scheme of creative destruction may lead to sophistication. However, this is rather due to a rising risk. The reason behind it was humanity itself, creating a problem from one side, and suffering to find a solution in another. This scheme portrays the excessive drain of human capital that remains ongoing in terms of militarization, and the rising cost of defense which would eventually lead to obsoletism.

C) O-ring influence and misplanning

The O ring theory was developed by the economist Michael Kremer back in 1993 to explain the overall inequality of expertise and the distribution of know-how across nations. It revolves around the fact that a product goes by many people and adjustments in order to get finalized and enter the market. However, if one entity fails to do its job, then the whole product becomes defective. Each one of us possesses a certain probability of achieving a task successfully, and the higher the higher expertise we get, the higher this probability. This most likely explains the university influence on wages, as in the higher the ranking, recruiters would assume a certain probability of success and thus their expected return would increase.[49]

Not to be outdone, the O ring theory has explained the difference in wages and why specialization has a positive correlation with wage. Let's take the example of manufacturing a car. It has to get sketched first of all, then go through the process of getting its pieces, its program, design, marketing etc… However, if one person failed to achieve their task, then the whole car would be defective. As they say a chain only is as strong as the weakest link. And that is exactly where cyberwarriors bet their expertise on. The O ring theory is not only applicable to commodities, but also in terms of strategy.

---

[48] **Periodica Polytechnica (2025).** "The Economic Measurement of Cyber Incidents: SolarWinds Analysis."

[49] Kremer, Michael. "The O-Ring Theory of Economic Development." *The Quarterly Journal of Economics* 108, no. 3 (1993): 551-75.

A war strategy is the reflection of various processors coming together to plan and gain momentum. Consider the following simplified model of the process, with the pager attack exemplification, we can take into consideration the Axis of Resistance point of view.[50]
The different phases of the military campaign would revolve around many tasks to achieve, each one of them would have denoted a certain probability of achievement, which is higher with accumulation of expertise.

1) Planning (*p)*
2) Artillery *(a)*
3) Communication (*c)*
4) Execution (*e*)
5) Support grant (*s*)

Note that this is a simplified model, there are obviously more phases that go around to achieve a great warfare plan. However, taking our onus into account, the whole idea around the O-ring is that all the different phases must be satisfied to have a successful military campaign. All in all the probability that the Axis of resistance would win is

$$\Pi\, pi -> p * a * c * e * s$$

However, what happened with the pager attacks is that communication was disrupted, with minimal effect in this case, causing the overall plan to crumble. This can be interpreted as a decrease in c to a near 0 value, meaning that in this case.

$$\Pi pi = 0 \; since \; c = 0 \; then \; p * a * c * e * s = 0$$

As the overall hybrid warfare caused a disruption within only one sector, it led to the overall plan to fall. As they say, a chain is only as powerful as its weakest link. Hybrid war has led to the vulnerability of many nodes within a plan, and causing higher risk of failure, thus extra damage and a longer timeline within war. However, risk can only be assessed within aversion, which would fall under the next part. [51]

[50] *The New York Times*, "How Israel Built a Trojan Horse of Pagers and Walkie-Talkies," September 18, 2024.
[51] R*euters*, "Hezbollah pager blasts: How the sabotage unfolded," September 20, 2024.

D) Risk aversion and Backward induction: Game theorizing hybrid warfare:

Now let's implement a decision tree within the new era of warfare. Bringing back the nuclear bomb incident, no one dared to wage war against Nuclear weapon holders due to the high risk of total destruction. Notably, hybrid warfare seems to follow this scenario. It is safe to assume common rationality here. Governments do not wage war randomly, but predict a certain outcome or expect a certain win.
After the full development of StuxNET by the US and Israel in 2010, the world held its breath with what they qualify as the '1st world cyber weapon' which reflects rather a risk aversion towards waging war with them. [52]
The emergence of hybrid warfare led various nations to think twice about waging war. Intelligence gatherings and major incidents portrayed how discrete an opponent can become, and a lesser payoff of winning, which in many cases is less than the payoff of not doing anything at all.

Case Study: The SolarWind Hack

According to the US government, the widely used Solarwinds has been hacked by blackhats affiliated with the Russian Intelligence Unit. The Biden administration authorized a cyber attack on both Russian and Chinese units, which resulted in an increasing fear and stalemate between the two opposing camps.[53] In May 2022 Gen Paul Nakasone confirmed that the US had many cyber attacks against the Russian bloc. The solar wind attack could be one possible reason why the US has insisted so much at banning TikTok from its territories. Silicon Valley and The Pentagon were widely affected by the SolarWind hack, which reminds us of the O ring theory. However, the larger scale became clearer: HybridWar does not only affect the physical battleground, but also the overall stability of the country, which is affected by various variables. From economics to politics, to media, and data collection, it seems that HybridWar may break the chain on all scales.[54]

---

[52] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2014.
[53] U.S. Department of the Treasury. "Treasury Sanctions Russia for Interfering in U.S. Elections and Conducting Cyberattacks," April 15, 2021.
[54] *Sky News*, "US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command," June 1, 2022.

Case Study: Cryptocurrency and the Wannacry

The Wannacry ransomware became a major shifter of cryptocurrency devaluation in 2017. As major Nato members blamed the Lazarus Group of North Korea for launching it, it injected itself in various files, which can only be opened after paying a ransom. According to the US and the UK, the Wannacry ransomware was supposedly helping raise funds for the DPRK, as they can purchase more and more military weapons through the collection of ransoms. However, the implications on the crypto market skyrocketed.[55]

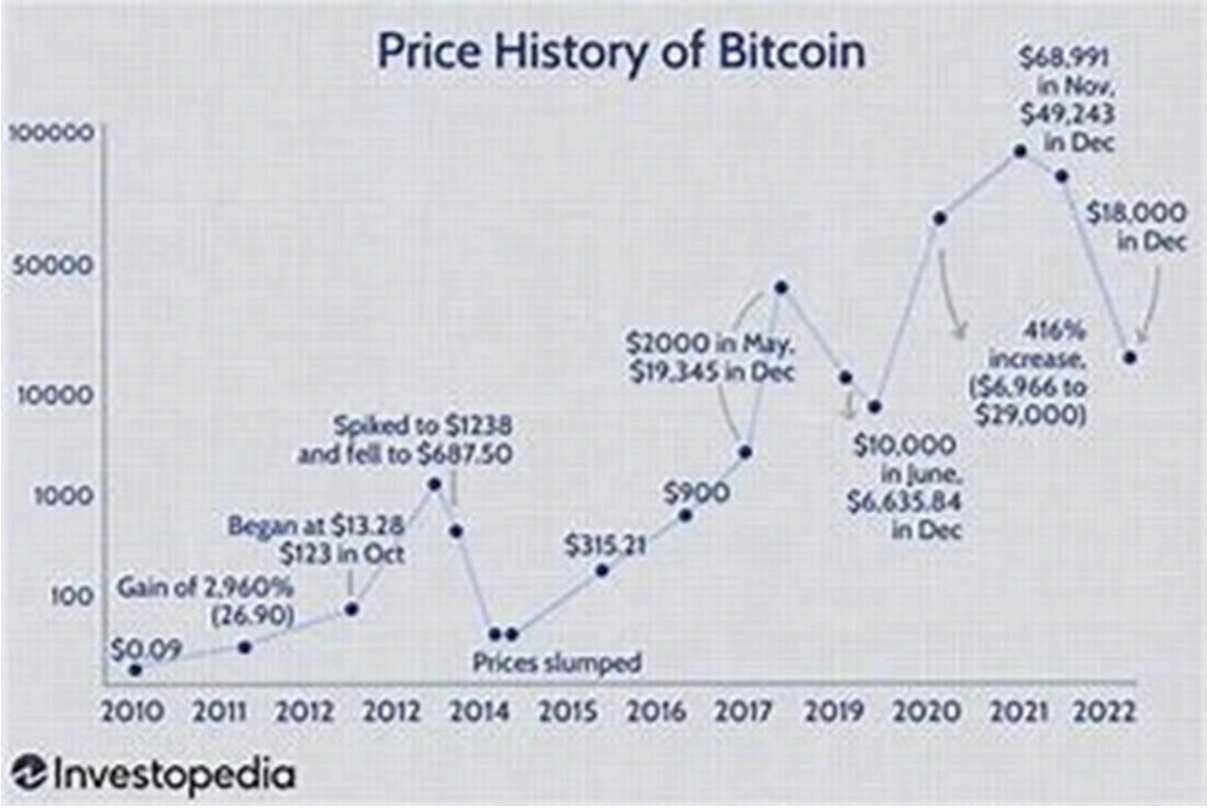


Figure 2.4: Price History of Bitcoin, Investopedia

Checking the price of bitcoin, by late 2017, we can witness that its price reached an all time high. After the British researcher Marcus Hutchins successfully neutralized Wannacry, speculation of getting stolen wallets became minimal. This led to a change of perspective in the crypto market, going from 6,000$ to 30,000$ in a matter of months. Other cryptocurrencies followed a similar pattern. [56]

[55] U.S. Department of Justice. "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks," September 6, 2018.
[56] *Wired*, "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet," May 12, 2020.

E) Bayesian Game: Incomplete information on one's type

Witnessing the picture of wars, we can already witness a rather bluffing that comes from here and there. Even the United States, currently considered the largest military power in the world, backs down from great conflict. Not because they are scared of losing, but rather of the losses that a war might commit. It comes in with a cost and benefit analysis.

If the country is a weak state, then the benefits outweigh the costs in that case, portraying why small nations go into coalitions together like the Caribbeans, Balkans, or even Pacific Archipelagos. However, no one is actually fully understanding how strong a nation is specifically. Portraying it within the Iranian-Israeli conflict, we can already see that Israel has rather underestimated the Iranian potential which led to the failure of the Iron Dome.

The move on whether to attack or not falls within a Bayesian game. Balcaen elaborated the inclusion of hybridwar within game theory. Let us think however, as a player who does not know exactly if the defender is weak (B') or Strong (B). [57]

[57] Balcaen, P. "Game Theory and Cyber Warfare: A Strategic Analysis of Information Asymmetry." *Journal of Cyber Policy* (2021).

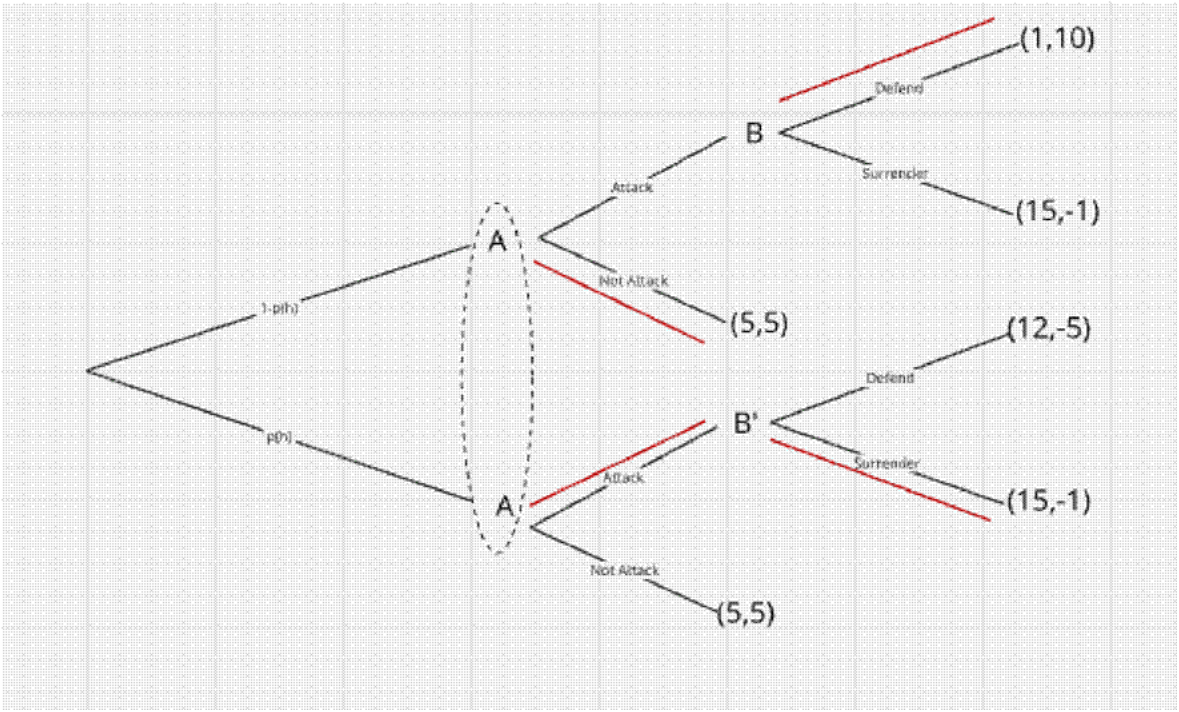


Figure 2.5: Theoretical Bayesian Game Tree

So Player A by not attacking would get by this tentative game tree a payoff of 5 anyway. However, the attacking move would be based on the beliefs, where attack

$E[x] = (1 - p(h)) + 15 * p(h)$ which must be greater than 5 in case individuals attack due to higher expectations.

$$(1 - p(h)) + 15 * p(h) > 5 \; then \; p(h) > 2/7$$

So the probability that he is weak with these values must be higher than 0.3 in order to attack, which might be unlikely in some large nations like Turkey, Indonesia etc…

However, in that case the usual scenario would be rather a decision not to attack due to risk aversion. In a case of hybrid warfare, the equilibrium could change completely. Imagine the scenario where the country is actually weak, and some spy network were able to decipher this specific fact. This would change the scenario to p(h)=1 and then attack.

p(h) would possess the following properties in that case

$dp(h)/dh > 0$ for weak nations as the higher the spy rate the more they lean on towards attacking

$dp(h)/dh < 0$ for strong nations as the higher the spy rate, the more they are averse towards attacking them.

The weak countries usually are the ones heavily investing in Butter as a percentage of their GDP, like Iceland, Cyprus, or the micronations of Singapore and Luxembourg. While these are known to have weak military, or no army at all, many nations keep their weaknesses hidden. Betting on the idea that the attacker is stuck in a Bayesian game, where it would be too risky to attack for them.

Hybrid warfare forces them to reinvest in guns, causing a drastic shift within the former model and investment in capital. This would potentially lead to technology drain. Although micro within the international scale, the nuclear curse seems to be showing up again, as the use of modern technology is only of use to destroy itself.

In conclusion, hybrid warfare is not only about breaking an opponent or not, but a rising discouragement of investment. The double edged sword that technological advancement holds cannot become more obvious. Our economy is separated into 2 large sectors, Guns and Butter. Utopically, the butter sector must have the larger focus, but due to a difference in technology progress, the Dutch disease manifests itself with the change in profits, and thus causing massive shifts and accompanying hybrid warfare with increase in gun production. We should also note that our digital era, despite its hyper-efficiency, is only a click away from being hijacked and disturbed. The rise of modern technology comes in with its own curse.

All in all, Hybrid war shifted the game theory, and rising dependency for comparative advantage and global trade in the world makes our production extremely vulnerable. One link is broken and the whole chain gets messed up. It is paramount to start digging more as we have already learnt our lessons from Ukraine, Taiwan, Lebanon and Estonia. Action is essential, and cybersecurity revisited, not only for the safety of the population, but also to spare another economic recession.

III) Political Repercussions and Analysis

The 21st century has witnessed a fundamental shift in the nature of international conflict. The binary distinction between war and peace has dissolved into a "grey zone" of hybrid warfare — a strategy that combines kinetic military power with cyber operations, economic coercion, and disinformation. As noted in the foundational definitions of the field, the objective is often to destabilize an adversary without direct physical confrontation, effectively "conquering the enemy without fighting." However, as digital connectivity becomes the backbone of economic and social development, the need for a robust strategy to ensure trust and security in cyberspace has never been more critical.

This essay explores the multifaceted nature of hybrid warfare, moving from the economic and technical mechanics of these conflicts to the complex legal and political frameworks attempting to regulate them.

III.1: The Mechanics of Hybrid Aggression

A) Economic Warfare and Supply Chain Vulnerabilities

Hybrid warfare targets the economic engines of nations. Modern production relies on globalized supply chains, which are governed by the **"O-Ring Theory"** of economic development. This theory posits that a supply chain is only as strong as its weakest link. If one critical component fails—whether due to a cyberattack or a blockade—the value of the entire production chain can drop to zero. In this context, "data blockades" have replaced naval blockades. For example, the disruption of satellite communications, such as the attack on Viasat in 2022, can sever a nation's industries from the global market, effectively strangling its economy.

Furthermore, the threat of hybrid warfare creates a **"Reverse Romer"** effect regarding investment. Technological growth relies on the expectation of future stability. When hybrid threats introduce persistent uncertainty, investors flee, and the depreciation of capital accelerates not due to physical wear, but due to the "obsolescence of safety."

B) Technical Tactics: From Wipers to AI

The tools of this warfare are sophisticated. Advanced Persistent Threat (APT) actors utilize diverse exploitation techniques that require defense-in-depth strategies. Key technical threats include:

- **Wiper Malware:** Unlike ransomware designed for financial gain, wipers (e.g., NotPetya, HermeticWiper) are designed solely to destroy data and cripple infrastructure.
- **Industrial Control Systems (ICS):** Malware targeting power grids and utilities poses a direct threat to civilian survival.
- **Artificial Intelligence:** The integration of AI into military decision-making creates new risks. While AI can process vast datasets for target selection, it introduces "automation bias," where human operators over-rely on machine outputs and "algorithmic bias". This can lead to discriminatory targeting in violation of humanitarian principles.[58]

III.2: The Legal Quagmire

As technology advances, international law struggles to keep pace. The anonymity of cyberspace and the involvement of non-state actors create a crisis of accountability.

A) The Attribution Problem and State Responsibility

Under international law, a state is only legally responsible for cyberattacks if those attacks can be effectively attributed to it. However, adversaries frequently use proxy servers, VPNs, and "false flags" to mask their identities.

- **The Evidentiary Burden:** To hold a state *legally* responsible requires a high level of evidence linking the act to the state, either through direct involvement or effective control over proxies.
- **The Proxy Gap:** Attribution criteria are historically based on conventional wars where states provided heavy weaponry to rebels. In cyberspace, non-state actors (hackers) are often self-sufficient and do not require state resources to launch devastating attacks, making the link to the state harder to prove.

[58] *The Guardian*, "The Gospel: How Israel uses AI to select bombing targets in Gaza," December 1, 2023.

B) Defining "Armed Attack" in Cyberspace

The United Nations Charter and the Law of Armed Conflict (LOAC) apply to cyberspace, but their application is contested.

- **The Tallinn Manual:** This academic study identifies 95 "black-letter rules" governing cyber conflict, addressing sovereignty and neutrality.[59]
- **The Schmitt Analysis:** To determine if a cyber operation constitutes a "use of force," experts propose analyzing its severity, immediacy, directness, and invasiveness. The law is clearest when a cyberattack causes physical damage, such as the destruction of an electrical grid.[60]

C) International Humanitarian Law (IHL)

IHL aims to protect civilians, but cyber warfare blurs the distinction between combatants and non-combatants.

- **Civilian Hackers:** A growing phenomenon involves civilian hackers participating in conflicts (e.g., the IT Army of Ukraine). The International Committee of the Red Cross (ICRC) has outlined **eight rules** for these actors, including prohibitions on attacking medical facilities, avoiding indiscriminate malware, and refraining from inciting terror.[61]
- **State Obligations:** States have a due diligence obligation to prevent civilian hackers on their territory from violating IHL and must prosecute those who commit war crimes via cyber means.[62]

III.3) Political Responses and Deterrence

---

[59] Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

[60] Schmitt, Michael N. "Cyber Operations and the Jus ad Bellum Revisited." *Villanova Law Review* 56 (2011): 569.

[61] International Committee of the Red Cross (ICRC). "8 rules for 'civilian hackers' during war, and 4 obligations for states to restrain them," October 4, 2023.

[62] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.
Jensen, Eric T. "Cyber Sovereignty and State Responsibility." *AJIL Unbound* 115 (2021).

Recognizing the limitations of international law, political bodies like the European Union and NATO have developed robust policy frameworks to build resilience and deterrence.

A) The European Union's Legislative Shield

The EU has moved from soft strategy to hard legislation to protect its digital sovereignty:

- **NIS2 Directive:** Mandates a high common level of cybersecurity across Member States, requiring implementation by October 2024.[63]
- **Cyber Resilience Act (2024):** Shifts responsibility to manufacturers, requiring products with digital elements to be "secure by design" and maintain security throughout their lifecycle.[64]
- **Cyber Solidarity Act (2024):** Aims to improve the detection and response to incidents across the Union.
- **ENISA:** The EU agency for cybersecurity has been granted a permanent mandate and increased resources to support certification and crisis management.

B) Sanctions and Deterrence

Deterrence requires that aggression be met with swift and credible punishment.

- **EU Cyber Sanctions:** The EU has established a framework allowing for targeted sanctions against cyber attackers. Notably, these political measures do *not* require the same high standard of legal attribution of international responsibility to a third state, allowing for faster political responses to threats.[65]
- **Nuclear Deterrence:** There is ongoing debate regarding whether nuclear weapons can deter strategic cyberattacks. However, given the difficulty of attribution and the risk of escalation, relying on nuclear deterrence for cyber threats remains legally and operationally fraught.

[63] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.
[64] European Commission. "Cyber Resilience Act: New EU Cybersecurity Rules for Digital Products and Software," 2024.
[65] Council of the European Union. "Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union."

C) NATO and Collective Defense

NATO acknowledges that a severe cyberattack could trigger **Article 5** known as collective defense. The alliance focuses on defining territorial boundaries in cyberspace and integrating cyber defense into its broader military doctrine.[66]

[66] NATO. "Brussels Summit Communiqué," June 14, 2021 (Paragraph 32 regarding Cyber Defense).

Conclusion: The Future of Hybrid Conflict

Hybrid warfare represents a permanent evolution in statecraft. It exploits the economic "O-Ring" vulnerabilities of globalization and the "Reverse Romer" fragility of investment markets, all while operating in the legal shadows of the "grey zone."

The response, as detailed in recent political briefings, requires a transition from reactive measures to proactive governance. This includes "humanizing" cyber war by applying Geneva Convention-style frameworks to digital conflicts,[67] enforcing strict product safety standards through legislation like the Cyber Resilience Act, and navigating the ethical minefield of AI-enabled warfare. Ultimately, the stability of the international order depends on the ability of nations to clarify the rules of engagement in cyberspace and enforce them through credible economic and political deterrence.

[67] Microsoft Digital Peace Now. "A Digital Geneva Convention to Protect Cyberspace," 2017.