Unraveling the European Legal Labyrinth of Technology Weaponization in Cyberspace

Sebastian Contin Trillo-Figueroa

LEXOLOGY

Unraveling the European Legal Labyrinth of Technology Weaponization in Cyberspace

China, European Union | August 30 2023

Mackinder's theory was stark: Control Eurasia, control the world. Spykman delved deeper, revealing that coastal dominance holds the key to global supremacy. Today, the battlefield has shifted from lands and oceans to cyberspace: Whoever reigns there, reigns over the universe. In light of this, global powers pursue digital hegemony through unconventional means, leveraging its unparalleled capacity to shape our existence.

Geopolitical Supremacy in the Age of Technological Weaponization

The weaponization of technology has transformed the interplay of geopolitical power. This paradigm shift intertwines innovation with strategic calculations, emphasizing the complex relationship between industrial policy, geopolitics, and the pursuit of competitive advantage and national interests. Consequently, a profound dichotomy emerges as leaders adopt divergent approaches:

- One positive, characterized by deep investments in strategic national technologies, aimed at reducing dependence on foreign suppliers.
- Another negative, which takes two protectionist forms: one directed towards rivals, employing trade measures to limit access to sensitive technologies; and another focused on fortifying security defenses against impending threats.

This dualistic interplay unfolds through the imposition of sanctions and commercial restrictions, where a balance is arduously crafted between high-tech advancement and self-preservation. As a consequence, the fragmentation of the global economy hampers collaborative efforts to tackle shared challenges and develop new technology.

5G: the Final Clash for Technological Supremacy amidst Legal Interference

The prominence of a specific tech protectionist aspect is related to fifth generation network deployment. The 5G race for supremacy presents a strategic opportunity for economic influence and technological leadership. Countries such as the U.S. express distress over the possibility to fall behind in the development of comparable equipment, particularly in comparison to China.

The stakes are high, as 5G networks are expected to play an unceasing role in supporting essential sectors and infrastructure. Given the growing recognition that cyberspace dominion equates to global control, concerns intensify. Additionally, since the Trump administration, the U.S. portrays Chinese dominance as part of a broader strategy aimed at challenging the global order and exerting influence.

Accordingly, Washington has developed a 'long-arm jurisdiction,' together with a narrative portraying Chinese authority in the wireless communication market as a Trojan horse. They argue that technological dependence, where critical components and equipment are supplied by dominant players, present security risks and the disruption of key services due to potential collaboration between companies and Chinese intelligence.

Essentially, the threat does not arise from direct evidence, but from Chinese data and network governance legislation that requires domestic tech companies to provide data upon request. The PRC National Intelligence Law mandates the 'platform economy' to "support, assist, and cooperate with national intelligence efforts […] and protect national intelligence work secrets they are aware of".

However, that prescription may appear naïve, as most countries, to varying extents, engage in metadata collection from their tech giants on national security grounds. In fact, the U.S., despite usually lacking specific legislation or authorizations, has employed extensive global surveillance initiatives through the National Security Agency (NSA). Programs like PRISM and Section 215 involve gathering internet communications from American big tech companies. Additional mass surveillance systems employed include Boundless Informant and XKeyscore. Furthermore, Snowden's revelations exposed the NSA's cyber espionage, encompassing hacking, offensive cyber operations, and the targeting of foreign governments and leaders like Merkel, Hollande, Rousseff, and Peña. Then, official leaked documents corroborated that it was the U.S. who engaged in espionage activities targeting Europe.

5G will cover all aspects of our life. Source: European Commission

Safeguarding the Rule of Law in EU Strategic Decision-Making

The question of whether the law is an equal boundary for everyone or becomes part of warfare is complex to elucidate in global powers' struggles. The U.S.' 'Entity list' and the subsequent Chinese retaliatory measures serve as evidence of this approach. However, in Europe, the rule of law is a sacrosanct principle, with separation of powers ensuring checks on authority. The EU emphasizes legal certainty for predictability and stability. Furthermore, Europe's regulatory influence extends globally, shaping norms and advocating for governance, justice, and accountability.

This comprehensive approach underscores the significance of law in European contexts, both domestically and internationally, serving as the foundation for formulating new norms. Nevertheless, a deviation from this path arises in the context of securing 5G networks. The introduction of the "EU Toolbox on 5G cybersecurity" in January 2020 signified a European shift, aimed to bolster security and reduce dependence on Chinese tech companies, aligning with Washington's narrative.

On June 15, 2023, the "Second report on Member States' progress" in implementing the Toolbox was used by the European Commission (EC) to limit research funding and contracts for "high-risk vendors" due to their "materially higher risks than other 5G suppliers." Only five days later, the EU doubled down introducing the European Economic Security Strategy, including further measures on the 5G/6G security.

Despite numerous expressions of dismay, no European institution has enforced a formal ban on networks to date. In fact, the current situation represents a reversal of the intended process. Ignoring the Treaty on European Union, particularly Article 26, which designates the European Council responsible for determining the common foreign and security policy, causes inefficiencies. Instead of ministers coordinating their national interests and the EU's highest officials implementing joint positions, the established protocol seems to be disregarded.

Moreover, implementing bans could potentially conflict with the principles outlined in the European Electronic Communications Code, which fosters competition, consumer protection, ensuring equal treatment for all providers. Similarly, once the rigorous certification requirements outlined in the Cybersecurity Act are met, challenging them becomes an overwhelming task.

Considering the widespread use of Chinese technology in Europe, any sudden changes must be well-justified, given the initial acceptance and traction gained. There are concerns from various institutions, often driven by politics rather than solid legality. Recent credible analyses illustrate setbacks from Huawei bans: UK's 5G lags, Germany's rail faces €400 million expense and 5-6 year delays, and Vodafone notes network quality drops due to unplanned tech exclusions. The question persists: Why profitable global companies would jeopardize their reputation for a government's benefit? The equation remains unsolved.

EU Measures Strongly Presented, Poorly Justified, and Timidly Delegated

The EU institutions have failed to assume their responsibility: recommendations on outlawing 5G networks have been strongly presented, poorly justified, and timidly delegated to the member states. When it comes to the development of the toolbox, compliance is only mandated through non-binding frameworks rather than enforceable legal measures. In straightforward terms, toolboxes and communications lack the regulatory power of regulations and directives.

EC's actions that encourage practices to exclude competitors for the benefit of others, based on invoked yet unproven security grounds, could be challenged under EU Treaties. The definition of the so-called 5G "high-risk vendors" needs thorough substantiation, appropriate regulation, and careful assessment and evidence to prevent damage to third parties who may sue, ultimately harming European consumers and the EU's reputation. Fair competition necessitates equal opportunities without double standards, discriminatory practices or country-specific policies that could be perceived as unfair.

The delegation of enforcing restrictions on high-risk suppliers to member states is inadequate if this issue is genuinely of strategic importance, as claimed, due to their limited capacity and potential consequences faced. Imposing a ban may trigger retaliation from China, a significant trading partner for many EU countries. This likely explains why, so far, majority of member states have passed legislation, yet it has not been implemented. In fact, the enactment process was supposed to be done by mid-2021, and is still ongoing. Furthermore, the European Court of Justice (ECJ) case-law requires that any national restrictions to rights guaranteed by Article 56 TFEU should be objectively justified and proportionate.

Hence, the EC should provide thorough justifications, a more unified, and a more coordinated approach, accompanied by an in-depth evaluation of the potential legal ramifications. National security is a sovereign matter, yet the Commissioner for Internal Market emphasized that their pressure is due to "a major risk exposing the Union's collective security," co-federalizing the issue. Any misstep that circumvents the law can be catastrophic, given the diligent oversight of the ECJ in upholding established norms. Looking forward, if any company perceives discrimination and if WTO rules or principles of free trade are violated, the absence of a viable mechanism to secure sufficient funds for substantial compensation could pose insurmountable future challenges.

Source: ECA, Special Report 5G roll-out in the EU, 2022. Exchange rates as of 31.12.2020

Challenges and Opportunities for the EU in the 5G Era

To effectively tackle these concerns, the EC should prioritize several key actions. Firstly, conducting a comprehensive assessment of potential distortions in the EU market and the subsequent impact on innovation: especially when the 5G Observatory Biannual Report (April 2023) reveals that among all member states, Sweden, Romania, Belgium, Estonia, and Latvia - the ones who preemptively banned Huawei -, rank at the bottom in 5G coverage. Secondly, addressing the economic aspect by conveying the inflationary pressure and the adjustment costs involved in replacing Chinese components, while finding alternative supply chains. Thirdly, leaders must clearly substantiate why alleged 'reliable' suppliers are never going to compromise the confidentiality of European metadata to their respective governments. Lastly, every explanation should be supported by solid evidence, adhering to legal frameworks, and aligning with the Union's core principles.

Because Europe is grappling with the urgent task of translating policy objectives into concrete legislation. Despite setting forth policies on issues such as data protection, cybersecurity, and digital rights, with the 5G toolbox there is a noteworthy gap between policy intentions and the enactment of robust legal frameworks. Simultaneously, while Chinese companies freely operate in Europe, EU businesses face substantial entry barriers in China, creating an unfair disadvantage that could weaken the legal claims of Chinese 5G tech companies. However, it is precisely in the 5G market, where Chinese authorities have displayed a higher level of openness, allowing European network vendors to secure a 16% share in a China Mobile contract.

Complexities might arise from disagreements in competences' distribution among EU institutions, potentially impeding effective resolution. Nevertheless, the EC has demonstrated remarkable agility in adapting more complex policies, as evidenced by the war in Ukraine, reducing dependence on Russian energy, and even controversial decisions like categorizing nuclear energy as green. Consequently, EU institutions appear to possess increased federal power, enabling more assertive decision-making processes.

Today's geopolitical battleground takes place in the cyberspace, where global powers vie for digital hegemony. There, the race for 5G has emerged as a pivotal clash, shaping the rivalry between the U.S. and China. As a consequence, the EU has been submitted to huge pressure, yet must preserve a degree of neutrality. Europe can position itself as a trusted intermediary, fostering open communication and cooperation between the two superpowers.

Furthermore, Europe's ability to maintain a delicate balance between political alliances (U.S.), trade relationships (China), and respect for the rule of law and legal certainty (own EU principles) is crucial. Providing a justifiable rationale for the aforementioned actions requires a careful and lawful narrative that highlights the imperative to safeguard economic stability, technological sovereignty, and national security in an increasingly competitive global arena.

China Legal Commentary Channel (CLCC) - Sebastian Contin Trillo-Figueroa