NATIONAL INSTITUTE FOR PUBLIC POLICY

INFORMATION SERIES

Issue No. 617 February 12, 2025

A Terrible Idea: Buying From Our Adversaries

Michael Hochberg
Michael Hochberg is a visiting scholar at the Centre for Geopolitics at Cambridge University, a Caltech-trained physicist, and a serial semiconductor company founder with four startup exits to his name. His writings on geopolitics can be found at longwalls.substack.com.

Introduction

Buying complex electronics and consumer goods from adversaries is a source of profound risk.[1] Electronics designed or manufactured in China can be an attack vector aimed at the United States. Changing tariff structures to 'price-in' the risk of such attacks, and to drive manufacturing away from our adversaries, is essential.

International Precedent

The recent Israeli pager attack against Hezbollah sounded a clarion call. It was a master-stroke of precision targeting, intelligence, and psychological warfare. Israel managed, in a single blow, to kill 39 people and injure nearly 3,000, representing the bulk of the middle management of Hezbollah.[2] Today, when one of Israel's enemies hears a phone ring, or turns on the car ignition, or presses the lever on his toaster, he surely experiences intense fear.

In developing their attack, the Israelis had a double challenge: First, they needed to turn the pagers into weapons. Second, they had to convince their adversaries to buy these weaponized pagers. The technical problem was likely the easier of the two.[3]

Creating a fake supply chain to insert these pagers into the enemy command hierarchy surely required operational genius. This operational problem was significant because

Hezbollah doesn't knowingly buy electronics from Israel: If it did, its members would have to assume that anything they were buying was an attack vector. This attack also pointed to the danger stemming from common U.S. consumer goods being manufactured in China.

Israeli Success Will Breed Imitation

Americans are too slow to recognize the danger of sourcing complex consumer and industrial goods from China. If China were to deploy a society-wide attack on the United States, it would face far fewer obstacles than the Israelis did when they corrupted Hezbollah's communication devices, because Chinese manufacturers are already deeply embedded in U.S. supply chains: A recent Federal Reserve report estimated that in 2022, 16.5% of U.S. imports came from Chinese sources.[4]

A steady increase in the volume of international trade – including specifically an increase in *de minimis* shipments valued at $800 or less – has made it progressively more difficult to detect malicious content in imported goods. There are as many as 4 million *de minimis* shipments to the United States every day; inspection of these daily shipments is infeasible. According to Andrew Renna, Assistant Port Director for Cargo Operations at John Fitzgerald Kennedy (JFK) Airport, "We have limited resources…there is no physical way…I could look at a significant percentage of that. So due to the volume, it's a very exploitable mode of entry into the U.S."[5]

Thus, incoming goods are often not being inspected at the borders for even very obvious hacks, like the insertion of explosives, because of the sheer volume of imports. Instead, only the most high-risk shipments are thoroughly searched; a recent audit of international mail processing at JFK airport found that even with this approach, enormous backlogs caused risky packages to slip through the cracks.[6]

While the mechanisms are new, targeted supply chain attacks are not. The United States has reportedly carried out its own supply chain infiltrations; in *At the Abyss: An Insider's History of the Cold War*, former National Security Council member Thomas Reed details a covert Cold War operation in which the United States inserted subtly hacked chips and equipment into Soviet supply chains by deliberately allowing corrupted parts to leak into Soviet hands, generating immense damage.[7] Attacks against the United States have already been observed as well.[8] At this point, any toaster or microwave being imported from China can contain an explosive, a hacked computer chip, or software or firmware containing back-doors.

These strategies are already spreading: Russia has been testing the use of incendiary devices shipped through commercial channels[9]. On the one hand, it is promising that this attack was detected before it was replicated at large scale, and that the origin of the attack was identified. On the other, this test attack was not detected until several packages had caught fire in Western countries.

The difference in scale between China-US and Russia-US exports is around three orders of magnitude. The scale of Russian exports to the West is comparatively small: For instance, Russian exports of electronics and industrial tools to the United States in 2021 were under

$500M in value,[10] and this number has almost certainly declined significantly since then. Keeping close tabs on this small volume of trade is comparatively straightforward. China's exports of electronics and machinery to the United States last year were over $200B and the exports by China-controlled entities from outside China are not included in this number.[11] For larger-scale attacks, prevention - or at least making such attacks significantly more difficult - is a far better strategic option than reprisal and escalation after an attack.

While this incident has shown that it is difficult for attacks like these to remain anonymous, it has also demonstrated that prevention is extremely challenging. Even in the Russian case - where trade volumes are modest, and Russia is widely known to be sponsoring terrorism and unconventional warfare - this test attack was not detected in advance and prevented.

Adversaries Are Aware of Dangers…and Opportunities

The fact that all of the world's advanced Central Processing Units (CPUs), Graphics Processing Units (GPUs), and Field-Programmable Gate Arrays (FPGAs) are designed in the West surely gives the Chinese, Russians, Iranians, and North Koreans great pause. Such chips are so complex that nearly any feature could be buried in their logic and remain effectively undetectable to any end customer.

That is why China has been desperate to take control of its high-technology supply chains, all the way down to the design and manufacture of the chips. The Chinese Communist Party (CCP) leadership recognizes the danger of importing chips and other critical components from its adversaries.

The United States must now appreciate that importing anything containing an integrated circuit or a complex circuit board from China threatens national security. While the Department of Defense has put a lot of attention on eliminating dependency on adversary supply chains, consumer goods have not received similar attention. Even seemingly simple products - say a toaster or a microwave - include non-trivial chips and circuit boards, and these circuits can conceal hacked chips. "Smart" appliances typically include an entire computer.

Some progress on this issue is already in motion: In August 2023, the Biden Administration issued Executive Order 14105, which sought to address reliance on foreign technology imports; the latest rules governing U.S. technology transfers with "high-risk" countries – most notably, China – include investment restrictions and export controls.[12] But these restrictions are limited in scope and fail to address the myriad challenges at hand. Digital hacking, surveillance, and targeted assassination with embedded explosives are only the tip of the iceberg: It would be quite easy to insert software into a smart, digitally controlled gas stove that opens the gas at a remote command, and then triggers a spark a few minutes later to ignite an explosion.

Almost any piece of consumer electronics could contain a bomb or could be designed to ignite an electrical fire on remote command. Malicious logic or analog functionality embedded in hardware, firmware, or software is very nearly impossible to detect if it is done with any level of finesse. Detecting this kind of "extra" feature – known as a "hardware trojan" if implemented at the chip level – is legendarily difficult, and doing so is a topic of active

ongoing research. It is effectively impossible to detect these types of hacks, except in truly extraordinary circumstances, without precise intelligence, access to source code, and design files. It is incredibly difficult even with such access, and it is hard to know that the design files and source code actually correspond to the final product; false design files or source code that obfuscate hardware or software trojans are comparatively easy to generate.

Batteries in cellphones, laptops, scooters, and electric cars are particularly dangerous, because they store a lot of energy and are easy to ignite, even by accident. Once these batteries overload and begin to burn, they are nearly impossible to put out, and a nefarious actor could remotely trigger an overload. Imagine if a million batteries across the country simultaneously caught fire one night.

Traditional Chinese strategic culture emphasizes the importance of unconventional warfare. Polluting U.S. consumer supply chains gives the CCP an opportunity to create problems for the United States at time of China's choosing. *The Thirty Six Stratagems*, a collection of Chinese proverbs, is illustrative, here: Stratagems 7 and 10, "Create something from nothing" and "Conceal a dagger in a smile," suggest creating chaos from seemingly harmless or friendly objects. In the modern world, batteries and cell phones exemplify such objects.[13]

No practical inspection regime could prevent such attacks, even with good intelligence backing it up. The cost of detecting trojans and other hacks is too high, and the skill base for doing so is too thin. The strategic cost of importing these kinds of goods from China, which has repeatedly declared its hostile intentions toward the West – and the United States in particular – creates too much vulnerability.

Reducing the Danger

The United States should incentivize companies to move manufacturing and design out of China to other nations that can build consumer goods at competitive prices, and that are allies or clients of the United States. National security is well worth the marginal premium; in practice, such a premium can only be imposed through policy means.

One positive step would be to require that all goods sold in the United States report what components were built or designed in China, Russia, Iran or North Korea or by companies controlled by these regimes. This would enable U.S. consumers to filter out anything manufactured in China from their purchases, which could in turn affect a larger shift in production toward domestic or allied sources.

The Trump Administration should raise tariffs on imports from China not solely to compensate for CCP subsidies to their industries or to enhance domestic competitiveness, but also to reflect the strategic danger created by imports of complex goods – including consumer electronics, chips, and industrial machinery. The United States should also subject Chinese client states and CCP-controlled companies operating outside China to similar tariffs. The goal should be to ensure that even small amounts of China-sourced content become uncompetitive for American customers. Chinese labor is not the cheapest in the world, and there are many

other states that want the business.[14] Relatively modest tariffs have huge effects – the modest tariffs of the first Trump administration were associated with a huge manufacturing and property boom in Vietnam, Thailand, and Malaysia, for instance, as Chinese companies moved manufacturing or finishing off-shore.[15] At the same time, the Administration ought to launch a strategic communication effort to explain China's dangers for U.S. national interests and economic prosperity.

Conclusion

The United States should subject the China and CCP-controlled companies operating abroad to prohibitive tariffs, not on economic grounds, but on national security grounds. Tariffs need to be set high enough that market forces drive demand away from China and Chinese companies, either on-shore or toward our allies. Similar programs should be implemented for other adversary regimes. The federal government should use tariffs as a mechanism for pricing-in the strategic risks and costs of importing manufactured goods from adversaries. These risks have been widely under-estimated.

To minimize domestic disruption, tariffs will need to be rolled out over time, starting with the most important goods and impacting the lower-risk products later. In the meantime, American consumers should consider that their purchases from China and other adversarial regimes may create direct physical danger for themselves and their families.

[1] U.S. Department of Defense, *Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order* 14017 (Washington, D.C.: Department of Defense, 2022), available at https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

[2] "Who was Hassan Nasrallah, the longtime leader of Hezbollah assassinated by Israel?," *PBS NewsHour*, September 28, 2024, available at https://www.pbs.org/newshour/world/who-was-hassan-nasrallah-the-longtime-leader-of-hezbollah-assassinated-by-israel.

[3] Sheera Frenkel, Ronen Bergman, and Hwaida Saad, "How Israel Built a Modern-Day Trojan Horse: Exploding Pagers," *The New York Times*, September 18, 2024, available at https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html.

[4] Trang T. Hoang and Gordon Lewis, "As the U.S. is Derisking from China, Other Foreign U.S. Suppliers Are Relying More on Chinese Imports," FEDS Notes, *Federal Reserve Board*, August 2, 2024, available at https://www.federalreserve.gov/econres/notes/feds-notes/as-the-u-s-is-derisking-from-china-Other-foreign-u-s-suppliers-are-relying-more-on-chinese-imports-20240802.html.

[5] Marcy Mason, "Buyer Beware: Bad Actors Exploit De Minimis Shipments," U.S. Customs and Border Protection, available at https://www.cbp.gov/frontline/buyer-beware-bad-actors-exploit-de-minimis-shipments.

[6] Department of Homeland Security, Office of Inspector General, "CBP Challenges in its Inspection Processes and Physical Security at the JFK International Mail Facility," March 12, 2021, available at https://www.oig.dhs.gov/sites/default/files/assets/2021-06/OIG-21-27-Mar21-Redacted.pdf.

[7] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine Books, 2004).

[8] "The Big Hack: How China used a tiny chip to infiltrate America's top companies," *Bloomberg*, October 4, 2018, available at https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?embedded-checkout=true.

[9] David E. Sanger, "Biden Aides Warned Putin as Russia's Shadow War Threatened Air Disaster," *The New York Times*, January 13, 2025, available at https://www.nytimes.com/2025/01/13/us/politics/russia-putin-airplane-shadow-war.html.

[10] "Russian Exports to the United States 2021," *Trading Economics*, January 2025, available at https://tradingeconomics.com/russia/exports/united-states.

[11] "Chinese Exports to the United States 2023," *Trading Economics*, January 2025, available at https://tradingeconomics.com/china/exports/united-states#:~:text=China%20Exports%20to%20United%20States%20was%20US%24501.22%20Billion%20during,COMTRADE%20database%20on%20international%20trade.

[12] Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," *Federal Register*, November 15, 2024, available at https://www.federalregister.gov/documents/2024/11/15/2024-25422/provisions-pertaining-to-us-investments-in-certain-national-security-technologies-and-products-in2.

[13] Davia Temin. "Ancient Wisdom For The New Year: The 36 Chinese Stratagems For Psychological Warfare," *Forbes*, September 25, 2019, available at https://www.forbes.com/sites/daviatemin/2017/01/02/ancient-wisdom-for-the-new-year-the-36-chinese-stratagems-for-psychological-warfare-in-business-politics-war/#:~:text=An%20adjunct%20to%20Sun%20Tzu's,they%20made%20my%20skin%20crawl.

[14] Sheera Frenkel, Ronen Bergman, and Hwaida Saad, "How Israel Built a Modern-Day Trojan Horse: Exploding Pagers," *The New York Times*, September 18, 2024, available at https://www.nytimes.com/2024/09/18/world/middleeast/israel-exploding-pagers-hezbollah.html.

[15] Zhenwei Qiang, Yan Liu, and Victor Steenbergen, "An Investment Perspective on Global Value Chains," *World Bank Group*, 2021, available at https://documents1.worldbank.org/curated/en/308861620996811293/pdf/An-Investment-Perspective-on-Global-Value-Chains.pdf.

The National Institute for Public Policy's *Information Series* is a periodic publication focusing on contemporary strategic issues affecting U.S. foreign and defense policy. It is a forum for promoting critical thinking on the evolving international security environment and how the dynamic geostrategic landscape affects U.S. national security. Contributors are recognized experts in the field of national security. National Institute for Public Policy would like to thank the Sarah Scaife Foundation for the generous support that made this *Information Series* possible.