Export Controls in an era of Strategic Competition:

Sectoral Guidance

CNS
Washington, DC Office

NONPRO NOTES
Sept 2022

Middlebury Institute *of*
International Studies at Monterey
James Martin Center for Nonproliferation Studies

James Martin Center for Nonproliferation Studies

Middlebury Institute for International Studies at Monterey

1400 K Street, NW, Suite 1225, Washington, DC 20005

Phone: +1 (202) 842-3100

www.nonproliferation.org/dc

This document was author by Dr Ian Stewart, Cameron Henderson and Eric Woods with input from Robert Shaw. It draws on research undertaken by a larger CNS team.

Cover image: "Flags of China, United States of America and Russia, gloomy clouds in the background, blurred image, 3D illustration, Milan Adzic". Available online at: https://www.shutterstock.com/image-illustration/flags-china-united-states-america-russia-1767631118

Executive Summary

This document contains sectoral guidance prepared by the James Martin Center for Nonproliferation Studies in relation to export controls in an era of strategic competition. The document is not a traditional report. Instead, it is a compilation of materials that will primarily be disseminated through other means such as online, through presentations, and through video. This executive summary section will not appear in other forms of this guidance. The guidance includes seven main sections.

First, the Introduction frames the problem and provides context into the work CNS undertook to produce this guidance. Second, the section 'Strategic Competition', provides insight into how great power competition is impacting export controls with an emphasis on Russia and China. This section also includes illustrative case studies for each country. Third, the section 'Trends in Technology Acquisition' outlines different methods being used to acquire foreign technology. This section includes a table of trends by sector and acquisition methods broken down with China and Russia specific considerations. Fourth, the section 'Sectoral Analysis' briefly examines several emerging technology areas. This section presents a summary of CNS sectoral mapping (and supply chain mapping) efforts research to identify sector-specific compliance considerations and risks. Fifth, the section 'Red Flags' presents red flags identified in the preparation of this guidance broken down by category to help inform due diligence efforts. Sixth, the section, 'Compliance Guidance' presents good practices in due diligence broken down into a number of thematic areas, including Company/Partner, Nature of Technology, Transaction, and Dealing with Academic Institutes. Additionally, this section includes Additions to ICPs and guidance on the Use of Distributors. Seventh, the Conclusion section briefly summarizes key takeaways from this work.

In addition to the seven main sections, the sectoral guidance also includes three annexes.

The first contains case studies. More than 30 case studies were written in the preparation of this report. The case studies are used to highlight key trends and tactics of technology acquisition elsewhere in the guidance. It should be noted that in the course of this research, CNS also used a data centric approach to map out the strategic supply chains of Russia and China. While this sectoral guidance is consistent with the observations gleaned from this data, the research team decided not to directly publish this underlying data as part of this sectoral guidance relying instead on the case studies. The reason for this is that some of the data sources will continue to provide insight into Russian and China's technology acquisition in the future. The research team nonetheless intends to publish more case studies drawing on this data in the future.

The other annexes include links to further resources; guidance on advanced due diligence techniques; and a table breaking down the red flags by sector.

Table of Contents

Note: This document is a composite of sectoral guidance elements that will principally be delivered in different formats such as by video, presentation and online through a website. For this reason, the sections of this report may not flow in the way that a traditional report would.

Author's Note on the Perspective of This Guidance

This guidance is written from a 'western' supply chain perspective. It is informed by dialogue with industry and governmental officials from many western countries including in the US and Europe. For this reason, the document is not written from either a Chinese or Russian perspective. The authors recognize that the perspective of these countries on the topic of strategic trade control in an era of great power competition would differ. Indeed, both countries implement export controls which are likely in part intended to prevent strategic technologies originating in these countries from being used or misused in western countries. The authors are interested in exploring the perspective of Russia and China in relation to great power competition. However, this is not the purpose of the present guidance.

Introduction

Recent years have seen the emergence of 'Strategic Competition' between key states including the United States, the People's Republic of China and the Russian Federation (hereafter PRC or China and Russia for shorthand). This strategic competition has far-reaching consequences including in relation to Strategic Trade. In recent decades, export controls have largely focused on weapons of mass destruction proliferation. This has been complemented by the widescale use of targeted sanctions by the UN, EU, US and other individual states. In the context of strategic competition, the focus of controls is evolving to be more focused on the potential use and misuse of technology to support military and strategic programs in what is described as resurgent great powers.

In this context, CNS undertook to identify what new needs governments and the private sector must meet to manage the risks associated with strategic trade. CNS specifically sought to examine these topics through the lens of certain key sectors – often called emerging and critical technology sectors, including those listed below. CNS undertook a global sectoral mapping exercise in relation to the supply chains for these sectors. This sectoral mapping work sought in particular to understand the role of China and, where relevant, Russia, in relation to the sectors. As part of this work, CNS also sought to understand the indigenization efforts of those countries in relation to each sector. CNS thus also examined both licit and illicit procurement and acquisition methods associated with each country and each sector.

In addition to this, CNS held a series of industry roundtables with the purpose of gaining insight from the private sector about the trade control challenges and considerations that go along with strategic competition. CNS held three roundtables on 18 May 2021, 20 October 2021, and 25 March 2022. CNS also presented and received feedback on aspects of this work for governmental, private sector, and non-governmental audiences on more than a dozen occasions.

Russia's invasion of Ukraine in February 2022 came partway through development of this guidance. Overnight, the export control and sanctions landscape related to Russia evolved. More than 30 countries agreed to coordinated action to cut Russia off from global strategic supply chains. As a result, to the extent possible, this guidance accounts for the evolution of controls – and Russian efforts to evade these controls.

In addition to this work, the research team identified, collated, and analyzed large volumes of data on Russian and Chinese procurement approaches and supply chains. The research team decided against directly drawing on this data for this report as many of the data sources are expected to provide ongoing insight into the technology acquisition approaches of both countries. The research team ensured that the insights from this data centric analysis are in line with the case study-based analysis presented in this sectoral guidance. The research team intend to publish additional case studies drawing from this data in the future.

This guidance is presented in a number of different versions: as a report; as a collection of interlinked web pages; as presentations, and as a series of videos. Common to all of these formats are the central elements of the guidance which includes this introduction, an introduction to strategic competition, a section on technology acquisition trends, a section containing sectoral analysis, a list of red flags, due diligence guidance, a section on managing distributors, and a brief conclusion.

Strategic Competition

This section sets out the context of strategic competition and what implications it carries for strategic trade control.

Export controls are evolving. In recent years, US export controls in particular have been viewed as tools through which to manage the rise of a geographically assertive China. This has necessitated a broadening of controls from the traditional scope of the main international export control regimes to cover both additional types of technology and additional types of trade and technology exchange. For example, the US and latterly the EU are working to identify emerging and foundational technologies that should be subject to control.[1] Additionally, many countries around the world have moved to introduce foreign direct investment screening systems[2], student and visa vetting systems, and to reinforce traditional export controls by bolstering technology controls and introducing military end use controls which can be leveraged in a context of strategic competition.[3]

Russia's invasion of Ukraine in February 2022 created a new catalyst for action. Overnight, more than 30 countries introduced coordinated sanctions on Russia which included restrictions on the export of controlled technology to Russia. Over time, the scope of these measures has increased as Russia's military action has continued. While in practice the Russia and China context are distinct, the cumulative effect is to refocus attention on how to implement effective export controls against strategic rivals like Russia and China which can use the full apparatus of their states to acquire technology. That can mean use of their security, intelligence, and cyberespionage apparatus to steal western technology and evade trade controls.

This is a new type of challenge for regulators and industry. What's needed for effective export controls in a China and Russia context differs. Particularly now that Russia is subject to broad sanctions, the export licensing dimension of the Russia challenge is perhaps more straightforward than it has been in recent history (i.e., most transfers are prohibited and won't be granted export licenses). The China challenge is complicated including by the existence of China's so-called Military Civil Fusion (MCF) strategy which sees civil industries leveraged for military and strategic purposes. Indeed, as the sectoral analysis for key sectors such as aerospace demonstrates, there is effectively no separation between civil and military programs, with specific entities being responsible for both programs. In both cases, there are well resourced efforts to evade controls to acquire foreign technology.

---

[1] See for example, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

[2] See for example https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

[3] https://www.gov.uk/government/publications/notice-to-exporters-202217-military-end-use-controls-update/nte-202217-military-end-use-controls-update

China-Specific Context

This section introduces the China STC challenge related to strategic competition. China implements a 5-year S&T indigenization plan and a policy of military civil fusion. These points drive China's approach to technology acquisition with knock-on effects for western STC implementation

Due to the People's Republic of China's continued high level of state control in the development of its economy, the government has been able to leverage these mechanisms to achieve strategic goals. Through its policy of Military Civil Fusion (MCF)[4], the PRC can coordinate its commercial sector towards specific national security priorities in a more direct way than true market-based economies. This is documented in the country's Five-Year Plans[5] (with a specific plan for Science and Technology[6] that is most relevant to strategic sectors). These plans guide the policy for the next five years and set out priorities and methods for achieving strategic goals. Early plans even mention the need to develop nuclear technology to jumpstart their nuclear weapons program[7]. The PRC also assigns funding and responsibilities to industry in pursuit of technology acquisition and indigenization.

Previous examples of these documents outline which target technologies are being developed for indigenous capabilities and that indigenous capabilities themselves are a high priority. By leveraging what the PRC calls 'cluster development[8]' it can grow strategic industries more rapidly and with less redundancy by coordinating government and commercial research and development efforts. Cluster development specifically is the idea that advancements in one sector necessarily result in advancements in other sectors. While in free market systems, such as that in the United States, advancements also spillover to other sectors, the PRC's ability to dictate its economy through MCF means that, as long as it is pursuant to a strategic goal, the transfer and integration of new technologies and advancements in other fields are facilitated by the government.

In practice, many PRC strategic companies are involved in MCF efforts. Many Chinese company websites will include a communist party page. The websites in the past have also often included either a page on military civil fusion or a page on China's Belt and Road Initiative (BRI) which, while principally a foreign facing development program, is

---

[4]https://www.uscc.gov/sites/default/files/2019-11/Chapter%203%20Section%202%20-%20Emerging%20Technologies%20and%20Military-Civil%20Fusion%20-%20Artificial%20Intelligence,%20New%20Materials,%20and%20New%20Energy.pdf

[5] https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf

[6] http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm

[7] "The 3rd Five-year Plan (1966-1970)," China.org, http://www.china.org.cn/english/MATERIAL/157608.htm

[8] https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf

an equally important indicator that a Chinese company is closely linked to China's strategic objectives.[9]

It is important to note that while the PRC does have a broad MCF strategy, in practice many commercial entities are still operating separately from the government or military. This results in an intentional degree of ambiguity when it comes to enforcing controls geared at military end users versus civilian purposes. This ambiguity facilitates potentially dual-use items to be purchased by a domestic commercial institution that can later utilize that technology for a strategic purpose. This is not to say that every technology traded with a commercial Chinese entity does result in a military end use, however, the structure, laws, and norms within the PRC do require that these actors would work in support of the state if tasked to do so through forced technology transfer.[10] To combat this, business due diligence is necessary beyond the normal list-based or catch-all based controls, especially considering that many commercial entities intentionally obfuscate information about their connection to government, or more specifically military, funders. The China challenge is considered to be particularly acute at present in part because of certain recent Chinese action. These actions include, but are not limited, to the following and carry specific implications for controls:

- China is at least two decades into a military modernization program that sees China develop substantial military capabilities.
- China is engaged in territorial expansionism in the South China Sea, including the militarization of Chinese-made islands with the purpose of expanding Chinese territorial claims.
- China is engaged in substantial nuclear weapons build up and has little to no separation between its civil and weapons sector.
- China is engaged in a significant missile systems buildup and has no separation between its civil and space sectors.
- Credible sources have alleged that China is engaged in the systematic repression of the Uyghurs in the Xinjiang province.
- Some Chinese entities are engaged in forced technology theft and technology acquisition both for monetary reasons and in support of China's broader strategic objectives. This includes civilians seeking commercial gain as well as military or state-led initiatives to acquire foreign technology illegally.[11]

At the same time, the Chinese market continues to be a lucrative and important one and it is essential that trade restrictions not overly impede commerce and cooperation with

---

[9]https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf

[10] https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf

[11] https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?emc=na&_r=1&

China other than where absolutely necessary. This is thus a difficult balance to strike and requires a nuanced approach to strategic trade management with China.

There are China-specific typologies of technology acquisition which are detailed more fully in the Trends in Technology Acquisition section. In brief, China leverages every apparatus of the state to acquire strategic technologies from abroad. This includes commercial arrangements (procurements, buying of foreign companies), sending students overseas, recruiting foreign researchers, and the use of front companies posing as legitimate commercial entities. Additionally, the Chinese government operates a substantial cyberespionage capability that works to acquire strategic technology in targeted areas. Historically, this has included active participation by units of the PLA[12] as well as units of the provincial level State Security offices.[13,14]

Labor and the flow of human capital is one of the top priorities for the PRC's attempt to acquire foreign technology. In context, it is important to note that the PRC is heavily prioritizing indigenous capacity to produce these strategic technologies to eliminate reliance on foreign actors. In contrast to Russia, for instance, which is currently severely constrained by the impact of global sanctions, the PRC's strategy of indigenization would serve as a buffer for the potential use of future restrictions by minimizing reliance from foreign nations, namely western states. Because of this desire for autonomy, the PRC has put more emphasis on acquiring the know-how over necessarily any one physical good; thus, recruitment strategies, such as the Thousand Talents Plan, are more prominent.[15]

While the flow of people is generally harder to manage than the flow of controlled goods, the strategy by the PRC does reveal the presence of "chokepoint" technologies. These technologies are ones that, in context, the PRC cannot independently produce yet and may be a hurdle to being able to indigenously produce a larger system. One such example is the use of interconnect technology for scaling supercomputers.[16] While the PRC can produce many of the pieces, they will not be able to indigenously scale up the supercomputers to those of western standards until they gain access to that interconnect processor and semiconductor technology. The upside to this is that while these technologies are often the target of Chinese technology acquisition attempts, they do provide insight into specific areas where the PRC is funneling its resources domestically and allow for more tailored mitigation efforts by western producers.

---

[12] Ibid.
[13] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion
[14] https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal
[15] https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf
[16] CNS HPC mapping report findings.

The China challenge is distinct from the Russia challenge, which is detailed below. In the case of Russia, more than 30 countries have implemented sanctions as a result of that country's invasion of Ukraine. In the case of China, sanctions do remain in force since the Tiananmen Square incident in 1989 which includes a US, EU and UK arms embargo on the country. However, outside of those measures there are no internationally agreed prohibitions on exports to China. Instead, each country generally assesses potential transfers on a case-by-case basis. A significant number of transfers are stopped each year, but the number of stopped transfers is generally small in comparison to those that proceed. This approach means that China continues to be well integrated into the global economy. It also means that licit transfers can be as important to China as illicit transfers given that there is a good chance that any specific effort to acquire strategic technology through licit means could be successful. This is different from the Russia case in which it is more likely that licit transfers would be stopped. The resources required by countries and companies to conduct a case-by-case approach to managing trade with China is substantial.

Illustrative Case Study: Front Company for Submarine Engines

One instance that highlights a variety of different methods the PRC uses to acquire technology in an era of strategic competition is case study 12, the 2018 case of Shanghai Breeze Technology Co.[17] Due to the restrictions on licensing for mainland China, it has become a common practice for entities attempting to acquire American origin technology to transship the goods through Hong Kong. In turn, shipments headed for Hong Kong warrant additional due diligence.[18]

In addition to the front company in Hong Kong, there was a separate front being used to finance the transaction, Belt Consulting Company Limited, also in Hong Kong. Shanghai Breeze Technology had also coordinated for an individual to transship the vessels and engines to mainland China from Hong Kong once delivered.[19]

Fortunately, the plot was thwarted. This effort, however, does showcase a modern approach by the PRC to obtain foreign technology for indigenous reproduction. The usage of front companies, largely from Hong Kong, both for procurement of goods and for financing of transactions are distinct red flags that can inform the work of compliance professionals. In this case, Shanghai Breeze Technology also sought military-grade equipment when civilian submersible engines do exist. This further highlights the dual-use and MCF risks associated with certain transactions.

[17] https://www.justice.gov/opa/pr/chinese-national-sentenced-more-three-years-federal-prison-attempting-illegally-export

[18] Ibid.

[19] https://seawaves.com/?p=13221

Illustrative Case Study: German Engine Technology in PLA Ships Caption: Chinese warship in East China Sea[20]

An example that emphasizes how export controls can implicate strategic competition is Case Study 17, the 2021 discovery of German engine technology in warships of the Chinese navy. Two companies, MTU and a subsidiary of Volkswagen, the French branch of MAN, were implicated in a report by German media for the supply of marine diesel engines for the Luyan III class missile destroyers. MTU had also previously supplied engines for the Song-class of submarines.[21]

The media report also mentions the joint venture MTU had to produce engines in China until at least 2020. This further showcases how the PRC uses various methods of technology acquisition to secure strategic technology. The subsidiary of Volkswagen, SEMT Pielstick, also had previously on their website reported their manufacture of PA6 engines for a frigate fleet in China back in 2002.[22]

According to the companies, they are fully compliant with the dual-use designation requirements under German law. This alone highlights the need for due diligence beyond standard dual-use requirements. Legal compliance is not always enough to prevent all risks, such as reputational risks to companies from bad media coverage or national security risks from providing engines to China's rapidly modernizing navy. [23] In addition to the Chinese acquisition of this German engine technology, the development of this case extends into 2022. In the spring of 2022, Thailand placed an order for Yuan-class submarines from China under the assumption that the German

[20] Image from: https://en.wikipedia.org/wiki/Type_052C_destroyer#/media/File:PLANS_Changchun_(DDG-150)_20180420.jpg

[21] https://www.dw.com/en/german-engine-technology-found-in-chinese-warships-report/a-59740301

[22] Ibid.

[23] https://www.theweek.in/news/world/2021/11/07/german-engines-powering-china-warships-eu-arms-ban-torpedoed-by-dual-use-tech.html

engine technology would be included.[24] The use of German technology in military equipment to the PRC is prohibited following the Tiananmen Square incident in 1989. Reportedly, since MTU's refusal to send the engine to China, the construction of the submarine has been suspended.[25] While the PRC has offered to include their indigenous diesel engines instead, the Thai officials have rejected such an offer because the engines are not the same caliber as their German counterparts.

Russia-specific Context

This section introduces the Russia STC challenge related to strategic competition. It outlines Russia's general approach to strategic technology indigenization and acquisition including relevant case studies.

Russia is actively developing advanced military capabilities, novel weapons of mass destruction, cyberespionage tools, artificial-intelligence driven weapon systems, and a host of other technologies with military and strategic applications. Overall, based on past precedence, Russia can be expected to try to leverage every emerging technology that offers strategic advantage. That said, while Russia generally has strong research and development capabilities and a strong military industrial base through which to produce strategic technologies, the country lacks many of the prerequisite scientific and technical basis required for specific capabilities and is thus dependent on foreign-sourced technology, goods, and material in many areas. As a result of this, Russia leverages the tools of the state and willing participants to acquire technology from abroad. This means the use of Russia's intelligence services, but also Russian nationals inside and outside the country willing to collaborate. In practice this means that networks of Russian nationals are willing to open companies and front companies in the West to send technology back to Russia. These patterns of transfer have been consistent for years and are likely to only grow given the comprehensive export controls introduced against the country in 2022.[26]

Following the February 24,[th] 2022 invasion of Ukraine, the United States, Europe, and major non-NATO partners such as South Korea, Japan and Taiwan jointly tightened export controls against Russia in technology sectors.[27] In practice this means national licensing authorities will not be agreeing to licenses of sensitive technology goods to Russia for the foreseeable future. These new controls, in combination with broad sanctions making financial transactions with Russian entities extremely difficult, forms what is in effect a partial economic blockade of the country. Russia's leadership

[24] https://www.thedefensepost.com/2022/04/13/thailand-chinese-submarine/
[25] https://eurasiantimes.com/thailand-rejects-to-buy-yuan-class-subs-china-german-tech/
[26] https://www.justice.gov/opa/pr/russian-agent-sentenced-10-years-acting-unregistered-russian-government-agent-and-leading
[27] https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/fact-sheet-joined-by-allies-and-partners-the-united-states-imposes-devastating-costs-on-russia/

has acknowledged that their broader strategy of import substitution, which has been touted for years, did not achieve the intended goals. In a rare admission of failure, Russian dictator Vladimir Putin said at a May 26, 2022 meeting that "[domestic substitution] is not a panacea".[28]

Russia has spent almost a decade investing large sums of money into projects for domestic substitution and development of emerging technologies with little oversight.[29] The strategy counted on Russia's strong cadre of scientists and engineers being able to catch Russia up to the United States and China. This included everything from domestic semiconductor production to drones and quantum computers. Russia has made some progress in being able to manufacture more primitive drones and microelectronics, but government neglect[30] and a bad business climate[31] have limited[32] Russia's technological potential and ability to manufacture at the cutting edge.[33]

In lieu of this, Russian top leadership has planned trade with Asia, as China in particular would serve as a reliable source of goods formerly imported from Europe. Based on available data, this plan has not been nearly as successful as President Putin and his close advisers had envisioned.[34] Fearing secondary sanctions and loss of the more important American market, there is evidence—a significant number of Chinese companies have refused to continue their business with~~in~~ Russian entities.[21] At present, there has not been a wholistic or systematic investigation of this across the Chinese economy. There are loopholes for Chinese companies that want to stay in the Russian market. For example, AliExpress, China's ecommerce giant, has been able to stay in the Russian market by becoming a minority stakeholder in its Russian subsidiary and by claiming it does not do business with sanctioned entities.[22] The Chinese government has given words of support, but has provided little to no material support based on available open sources.[23]

The challenge posed by Russia is distinct from the challenge posed by China. Russia has a deep pool of strong universities and academic research centers that have been in place for a century. Rather than a rising country only growing further as a technological world power, Russia is attempting to provide its already world-competitive science and

---

[28] https://rg.ru/2022/05/26/putin-importozameshchenie-ne-panaceia.html

[29] https://www.youtube.com/watch?v=6dIjeUB51-s&ab_channel=%D0%90%D0%BB%D0%B5%D0%BA%D1%81%D0%B5%D0%B9%D0%9D%D0%B0%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9

[30] https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

[31] https://www.nytimes.com/2021/08/06/world/europe/russia-american-investor-calvey-sentence.html

[32] https://www.rferl.org/a/emigration_blues_russias_sixth_brain_drain/2294463.html

[33] https://www.themoscowtimes.com/2020/06/08/russian-investment-world-rocked-by-yet-another-criminal-case-a70507

[34] https://www.aljazeera.com/economy/2022/4/1/for-isolated-russia-replacing-key-imports-an-uphill-battle

technology base with the tools they need to succeed. The fear in Russian society caused by President Putin's war on Ukraine has caused tens of thousands of Russia's brightest minds to flee.[35]

To keep its scientific infrastructure stocked, Russia is reliant on foreign supply chains both licit and illicit.[36] This system will continue to operate, and has the potential to become more aggressive as the war forces Russia to rebuild military items.[37] The use of former Soviet republics such as Kazakhstan,[38] Kyrgyzstan,[39] Azerbaijan,[40] and Georgia[41] as transshipment points has become a point of concern.[42] These countries have accepted large numbers of Russians fleeing internal repression and looking for a connection to the outside world.[43] Invariably, these young states have limited capacity to monitor the myriad of informal and formal trade connections between their states and Russia.[44] Many of these countries are Russian allies and continue to be reliant on Moscow for their own economic and physical security.[45] Russia's defense base, knowing the weaknesses of domestic production will continue to find it necessary to procure the components they need to operate from abroad. The former Soviet republics in the Caucuses and Central Asia are ideal locations given geographic, linguistic, familial and economic ties to Russia. Additionally, Russia can credibly threaten these countries in policy areas important to Russia and has done so since February 24th.[46] Indeed, as the following case study demonstrates, Russia is reliant on illicitly acquired goods for its strategic programs and Russia has built up a substantial apparatus through which to acquire western materials, goods and technology.

Illustrative Case study: Chemical Weapons Supply Networks

[35] https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html
[36] See case studies 23, 24, 25, 27, 28, 29, and 32.
[37] https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html
[38] https://archive.ph/x8voi
[39] https://news.obozrevatel.com/economics/analytics-and-forecasts/visa-ot-kirgiza-kak-rossiyanam-pomogayut-obhodit-sanktsii.htm
[40] https://tass.ru/mezhdunarodnaya-panorama/15071735
[41] https://news.obozrevatel.com/economics/analytics-and-forecasts/rossiya-obhodit-sanktsii-s-pomoschyu-gruzii-na-granitsah-vyistroilis-ocheredi-iz-fur-video.htm
[42] https://www.kommersant.ru/doc/5380684?query=%D0%BA%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD
[43] https://www.rferl.org/a/russian-emigres-central-asia-ukraine-war/31883254.html
[44] https://thediplomat.com/2022/07/russias-war-puts-central-asias-economies-in-a-difficult-position/
[45] https://abcnews.go.com/International/russian-troops-begin-leaving-kazakhstan-government-restores-control/story?id=82243668
[46] https://korrespondent.net/world/4487555-putyn-obydelsia-na-kazakhstan-y-nachal-torhovuui-voinu

One instance that highlights the important role of international supply chains to Russia's security apparatus is Novichok nerve agents. According to scientists who worked on their development, this family of agents were developed by Russia from the 1970s to the 1990s at least partially for the Ministry of Defense.[47] The same substances have particular utility in relation to targeted assassinations carried out by Russia's security services. The agents came to international attention in 2018 when Russian national Sergei Skripal was targeted for assassination with the agent. The UK has blamed Russia for the assassination attempt and open source investigations suggest a Russian military team was deployed in the UK to carry it out. The substance gained greater attention with the failed assassination of anti-corruption activist and dissident Alexey Navalny. That failed assassination was carried out by a team from Russia's FSB.

It is believed that the key entities responsible for Russia's Novichok program benefited from the use of Western supply chains.[48] Companies, including Russian-connected companies in Germany and Switzerland acted as intermediary warehouses and fronts for the procurement of laboratory equipment and chemicals for entities sanctioned for their ties to Russia's alleged chemical weapons program. Investigative journalists at independent Russian outlet *Fontanka*, and confirmed by CNS, highlight several links between these sanctioned companies to the Russian government and relevant entities linked to Russia's alleged chemical weapons program.

Others, such as Riol Chemical, supplied chemicals to government contractors of Russia's security services, specifically Russia's Khimmed Group.[49] German investigators raided the offices of Riol Chemical in August 2022 as the company did not apply for the right to export the dual use chemicals.[50] Phone intercepts by German police allegedly caught company employees discussing strategies to hide the shipments. This included both using third parties to ship the goods and pretending that some were intended for Lithuania, a strategy the company previously used for illegally exporting special lab equipment to Russia.[51]

It is important to note that Russia's technology acquisition approaches are likely to change following its invasion of Ukraine. Licit transfers of strategic items from nearly

[47] https://thebell.io/razrabotchik-novichka-vladimir-uglev-partii-sostavlyali-ot-20-grammov-do-neskolkih-kilogrammov

[49] Riol Chemical supplied Khimmed Group, who then supplied Russia's military and intelligence services according to independent Russian outlet Fontanka. https://www.fontanka.ru/2021/03/05/69797849/print.html

[50] https://www.occrp.org/en/daily/16706-germany-raids-companies-that-exported-dual-use-chemicals-to-russia

[51] https://www.tagesschau.de/investigativ/ndr-wdr/durchsuchung-dual-use-101.html

anywhere in the world are now unlikely. Instead, Russia is likely to rely even more heavily on illicit means and to turn to other malign economies to support its programs.

Implications for Export Controls at the National Level

Strategic competition and Russia's conflict in Ukraine are likely to have important implications for multilateral export controls. Some have muted the possibility of creating new multilateral export control regimes to address these challenges, for example.[52] It is understandable that many states will not wish to take a position in relation to strategic competition *per se*. Regardless, states should ensure that they at least have instruments, systems and processes to provide visibility of potentially problematic transfers and cooperation with states such as Russia and China – and indeed any other country viewed as being of concern.

The toolset needed to monitor and manage strategic trade is different now than it has been in recent decades when the principal threats were non-state actors and so-called rogue states such as Iran, and North Korea. In the case of China, in particular, the country is so integral to the global market and supply chains that controls must be carefully calibrated so as not to unduly harm the implementing state. This said, at the same time, the aperture of what should fall within scope of controls is broader given the approaches to technology acquisition as detailed elsewhere in this guidance.

Export controls based on the existing regimes will not be sufficient alone to manage risks under great power competition. This is for a few reasons. Firstly, regime-based control lists have bureaucratic hurdles for modifications and additions which frequently lag behind the rate of innovation in tech sectors. Secondly, regimes are dictated by the actors engaging in strategic competition with each other, including Russia and China, potentially undermining the legitimacy of the regime's response to risks posed by its own members. Lastly, due to the number of acquisition methods being utilized to obtain strategic goods, states may need to take unilateral action to protect its domestic industry beyond standard export controls.

In this context, and in the course of the work to generate this guidance, CNS has identified the following elements that states should implement.

- Enact a military and strategic end use control which can be used in relation to Russia and China. Globally, the existence of military end use controls has generally lagged behind weapons of mass destruction end use controls perhaps because the latter is an expressed requirement of UNSCR 1540.
- Promulgate lists of entities of concern in Russia and China such that companies and financial institutes must refer cases involving such entities to authorities. In Russia, for example, it is known which institutes are thought to be involved in

[52] https://nonproliferation.org/export-control-and-emerging-technology-control-in-an-era-of-strategic-competition/

the Novichok program. And in China, it is known which organizations and institutes are involved in the nuclear weapons program (the China Academy of Engineering Physics) and missile programs (the China Academy of Launch Vehicle Technology). These lists of organizations include military linked universities, for example.

- Set out standards for cybersecurity of export-controlled information that technology holders and exporters must meet. Presently, few countries address the cybersecurity of export-controlled information.
- Ensure nonproliferation controls are being implemented in universities and research institutes. Consider implementing vetting and deemed export controls in pursuit of this objective. Presently, many countries do not have adequate controls in place to safeguard sensitive technology held in universities and research institutes. Furthermore, in many countries, these actors have not been adequately engaged with in regards to export controls.

Each of these elements is complex in its own right. In several areas, CNS has been working to develop additional guidance and training materials which may be added to the present guidance in the future as this guidance is expanded from its present private sector focus to a state-centric scope.

The trends and tactics being employed as a result of strategic competition also carry important implications for companies. The remainder of this guidance focuses on what companies should know and what additional due diligence steps should be taken by companies. This includes a section on trends in technology acquisition, a section on acquisition methods, a list of red flags, a section on due diligence elements, and a section on potential additions to internal compliance programs. Additionally, the guidance also contains a number of case studies and how-to guides.

Trends in technology acquisition

Parallel trends such as globalization, digitization of the economy, and technology advancement have collectively resulted in an increasingly rapid capability for technology to be innovated and disseminated. While largely these processes are positive, they do result in lower barriers to technology misuse by either states or non-state actors. Measures such as UNSCR 1540 in 2004, which requires all states to adopt export controls and other measures to prevent nonstate actor involvement in proliferation, were a recognition and embodiment of this challenge particularly to the extent that non-state actors were involved in technology diffusion for terrorism or weapons of mass destruction end uses. In the new era of strategic competition, it is clear that states have the ability to take advantage of technology digitization and diffusion to support their military and WMD end uses of concern.

In this context, and in addition to the Russia and China specific considerations set out in the previous section, the observable general process is for there to be less isolation between end uses and end users of concern and global supply chains. The process by which this occurs can be distilled into a basket of observable trends. 'Trend' is defined in this report as observable common techniques that Russia and China are employing to obtain foreign technology or expertise in strategic sectors.

This section begins with a table charting different areas of technology and various means of acquisition used by the two countries. After the table showing the relationship between different acquisition means and technologies is an explanation of the technologies themselves. After the sub-section on technologies there is a sub section exploring the commonalities and differences in acquisition by the two countries in greater depth.

For the purposes of this section, acquisition of strategic goods will generally be for either the completed goods (or components of goods) or for the means to produce these goods. That is, it could relate to a semiconductor device that is acquired from abroad or it could relate to a Chemical Vapor Deposition machine used in the manufacture of semiconductors. Some of the tactics that will be considered are relevant only for one or the other of these purposes.

The following table (Table 1) displays the presence of specific acquisition methods across strategic sectors. The table indicates where there has been an observable instance of technology acquisition to highlight trends where appropriate. The table does not preclude the possibility of various transfer methods in specific industries but is simply a heuristic for common instances that the CNS team has observed while undertaking our sectoral research

The trends shown in this table are built upon in the acquisition methods and sectoral analysis sections.

Table 1. Trends by Sector

	Machine Learning	Computing	Semiconductor	Composites	Genomics and Biotech	Aerospace and Hypersonics	Telecomms	Robotics and Drones	Other / general
Licit Purchases from producer	China	China	Russia	China, Russia		China	Russia, China		China
Purchasing on secondary market									Russia
Illicit Purchase via front companies			China, Russia			China, Russia		Russia	
University Collaboration	China	China	China	China	China	China, Russia	China		
Investment and company acquisition			China	China					
Cyber theft and cyber espionage		China	China		China	China, Russia		China	China
Recruitment of foreign experts			China	China	China				China
Misrepresent the contents or origin of packages			Russia			China			
Acquisition of production		China			Russia	Russia	Russia	Russia	

components **									
Acquisition of complete item			Russia						

Acquisition Methods

The acquisition methods across both countries use both licit and illicit means to obtain foreign technology or expertise in strategic sectors. The line between ordinary cooperation and harmful transfers is often the presence of state interest in the transfers. Technologies that can be used by militaries and intelligence services are highly valued and given the sensitivity of such acquisitions, illicit means using front companies, false assertions of end use, and general plausible deniability of government links are attempted. Thankfully for due diligence officers and companies, these patterns are generally less sophisticated than one may assume and often exhibit poor 'tradecraft'. As such, certain patterns emerge so that companies can identify transfers that may present financial, legal and reputational risks. This section first lays out the commonalities between the two countries with a discussion of mutual tactics for technology procurement. This section analyzes the different methods each country employs in a country-specific context. This section references case studies published as part of this guidance.

Common Acquisition Trends

Licit Purchases

Due diligence efforts undertaken by industry professionals and government employees focus most frequently on the illicit transfer of dual-use technology to a foreign country. However, it is the essence of dual-use goods to have legitimate uses as well. To leverage the legitimate uses of these goods to procure something that still has military implications, both China and Russia do acquire strategic technology legally including through open procurement. This specific method likely overlaps with other methods of acquisition where the reason for the legal exchange of goods is either fabricated documents, a dubious end-user hiding their intent, or due to joint or collaborative settings.

As seen in Case Studies 24, 25, 26, 27 and 28, a common tactic of acquisition for Russian entities is to licitly purchase from abroad. This acquisition method can overlap with other methods, particularly the acquisition of production components from abroad. In Case Study 24, there is an example of this where there was a licit purchase of machinery to a Russian entity working on a hypersonic flight project. In Case Study 25 we see the example of calibration devices sold by an American company and then sold on again to the Russian security services. In Case Study 26 we see the sale of a convection oven for production of electronics from a German company to a Russian defense entity. These licit sales are often associated with European companies selling to Russia's military industrial base or intelligence services, German companies in particular.

Due to the Military-Civil Fusion strategy being employed by the PRC, many dual use purchases which are seemingly benign in nature may end up with linkages to Chinese

military or strategic institutions. Licit purchases end up having dual use implications in a Chinese context commonly in university settings. One example of this is in case study 16 when a joint project on a quantum communications network between an Austrian university and a Chinese university resulted in the development of dual-use quantum encryption network in the PRC using multiple American sub-components. While these cases may be less prevalent due to the due diligence of industry representatives, there is a need to apply similar due-diligence measures to educational or joint venture settings in a Chinese context to prevent the misuse of licit purchases. Additionally, case study 17, wherein German companies provided marine diesel engines to the Chinese navy, showcases that legal compliance with export controls on dual-use technologies is not always enough to prevent risks to reputation of the company involved or risks to national security.

Illicit Purchases via Front Companies and Intermediaries

One of the most common methods to acquire foreign technology illicitly is using front companies or other intermediaries to transfer goods. While this can look different depending on the context, the general allure for this method is to use a front company in a location that is less likely to receive scrutiny when applying for a license of a controlled item. Front companies can be used for financing, transfer, and reshipment, so it is important that due diligence efforts adequately screen for these cases, paying special attention to the geography of the buyer.

As seen in Case Studies 18, 19, 21, 22, 23, 30 and 31, a common tactic to procure goods is the use of front companies and intermediaries, particularly for Russia. The use of fronts and intermediaries, such as freight forwarding and nominal wholesalers, can mask when a good is destined for a defense industrial entity or defense research center. These networks can be familial as in the Brazhnikov case (Case Study 19), but do not necessarily have to be. As seen in the Fishenko case (Case Study 23), companies engaged in illicit exports via co-conspirators running front companies or intermediaries abroad can operate for years depending on their level of sophistication and operational security.

The PRC uses several front companies to transship goods to mainland China. The main reason for this is the distinct licensing requirements between the PRC and surrounding areas which are trading hubs, such as Hong Kong, Macau, or Indonesia. There have even been criminal cases where the defendant has revealed that they are trained to transship into Hong Kong to be more likely to get a license approved, as was the case in the investigation of Shanghai Breeze (Case Study 12). Front companies have been used in the Chinese context both as a transshipment hub and an alternative financing scheme to obfuscate government connections, which was also highlighted in the Shanghai Breeze case study for using a secondary front company in Hong Kong to finance the purchased goods. For that reason, it is important to be aware of instances where the financing company may be different than the front company being used as a shipping destination.

Misrepresentation of Package Contents

One strategy both Russia and China can employ to acquire technology is to misrepresent the contents of a shipment. This can either be done intentionally by a seller attempting to make a transaction without a license or unknowingly by an employee of the company acting alone. These instances can be hard to catch as recruitment of personnel within companies is hard to track. Additionally, customs officials may not be adequately trained in identifying specialized equipment to be distinct from what was claimed to be sold.

As seen in Case Study 22, the Flider Case, when transferring packages containing controlled goods the seller wrote 'power supplies' on the package. By labeling the packages as power supplies, spare parts or other goods, the seller is attempting to make the package not raise the suspicions of customs or border officials and avoid inspection.[53] The use of 'power supplies' in that instance preys on the fact that many customs and border officials are undertrained and are not capable of recognizing many dual use goods. In the event the package is inspected, the average customs official would not necessarily be able to differentiate power supplies from another electronic good. This is a common smuggling technique for small components and is likely much more widespread, but given the nature of the data on this, it is difficult to map how extensive it is.

Misrepresenting the contents of a package frequently requires an insider within the company of interest to be able to fabricate documents for the exchange. Thus, to understand how the PRC utilizes this method, it is important to consider it in the context of their broader foreign recruitment strategies and the role of the Thousand Talents Plan. Specific examples have included case studies 2 and 7 wherein representatives working at companies in the US forged documents as well as used insiders at foreign subsidiaries of American companies to misrepresent the package at the transshipment destination in the country the subsidiary was based in.

Acquisition of Production Components

In assessing the various methods of technology acquisition, the research team found there was value in analyzing both the acquisition of equipment used in the production of strategic technologies and the strategic technology itself. This distinction can glean insights about the chokepoint technologies that the PRC and Russia are most reliant on foreign partners for or which technologies the countries are trying to indigenize. Certain sectors, such as additive manufacturing, are more easily defined as components versus completed items. In a completed item, the product is fully manufactured and sold as one item. Component pieces are the items required for the construction or manufacture of the aforementioned item. In sectors such as semiconductors, it is

[53] https://www.smallarmssurvey.org/sites/default/files/resources/SAS-IB17-Mechanics-of-trafficking.pdf

harder to pin down because the finished product of the semiconductor will be only a component in a broader piece of equipment for another industry. For this reason, this section prioritizes those components that are utilized for a separate end-use or used in the production of a strategic product.

In Case Study 31 CNS discovered that poison labs run by the Russian government were purchasing the components suitable for the creation of nerve agents from abroad. Given limits or constraints within Russia's own chemical industry, precursors required for the manufacture of these poisons was done from abroad. This meant the use of intermediary wholesalers and suppliers for dual use goods, that on paper had mundane applications as pesticides and other purposes but could also be used to create tools of assassination. This is also seen in Case Study 22, the Flider case, where microelectronics used for drones and potentially other sectors were procured from abroad. Russia, as discussed, is particularly reliant on the acquisition of production components from abroad given the idiosyncrasies of the country's industrial development. Acquisition of production components do not always have to be illicit. In fact, in the 2014-2022 time period, many Russian defense manufacturers licitly purchased production equipment from Italian and German companies as seen in Cases Studies 24 and 26 This approach of focusing on acquiring dual use components is seen in a myriad of Russian cases. The nuances are explored in more depth later in this section.

Several things could be categorized as production components, but this section is simply to highlight that there are tendencies for the PRC to acquire or attempt to acquire an individual component rather than a finished product. In many cases, this is easier to do, but in the Chinese case this is largely due to the intent to be able to refabricate and indigenously produce strategic technologies. Many times, a single technological component is what is delaying the development of other scientific advancements, and in these instances, the PRC may target that instead. One such example in case study 1 is the theft of Micron's Direct Random Access Memory (DRAM) technology that is used to develop more advanced semiconductors, which in and of themselves are a component for larger supercomputers or aerospace devices. While this example was an illicit transfer, it is important to note that in other fields, such as advanced manufacturing, inputs for specific manufacturing devices with dual use implications should be considered. Namely, as new materials for additive manufacturing are developed with increased resistances or advanced properties, those inputs should be considered in the context of what the PRC industry can produce with them.

Cyber Theft

Given the digitization of the global economy and manufacture, cyber security theft and hacking are playing a particularly important role in relation to technology transfer at present. While most industries are applying cyber-standards and protections for their proprietary information against more common cyber-threats, advanced, coordinated hacking attempts such as those by Russia and PRC to obtain foreign technology persist.

The open-source literature on PRC use of this acquisition method is plentiful. The technique is so widespread there have even been two examples where provincial level (rather than national level) state security offices in the PRC have hired hackers and software experts to develop malware and advanced phishing techniques targeting a variety of industries and organizations.[54] These operations typically take place over many years and can involve several countries. Case studies 3 and 8 exemplify these. One included the Jiangsu Province Ministry of State Security (JSSD) and targeted aeroengine technology most specifically. The other involves the Hainan State Security Department (HSSD) and focused on a variety of sectors from genetic sequencing to submersible vehicle technology.

As cyber-attacks have targeted digital information such as chemical formulas, engineering schematic diagrams, and business information used to secure third-party contracts, industry leaders must prioritize the cyber-security of strategic information. This is particularly the case with Russia, where the intelligence services are known to target contractors working on aerospace and other military technologies.[55]

University Collaboration

As universities are hotbeds for innovation and research, many strategic technologies are jointly developed with universities, especially those that are receiving grants for government sponsored research. This is true of the United States but not to the same extent that MCF strategies in the PRC leverage these resources.

While there are examples where a Chinese university has collaborated with an American or other foreign university to develop a technology that can then be applied for dual-use applications in the PRC, such as is the case with the quantum telecommunications network technology, it is not the only form of strategic collaboration utilizing universities. Frequently, university collaboration takes place when a researcher from the PRC goes to a technology holding country to work or study at another university and performs research in a strategic field with the intent of returning to the PRC to advance their strategic sector. This can, and has, included instances where the collaborator was tasked with performing similar research for both American and Chinese government grants simultaneously. This is exemplified in the case studies 4 and 5 involving researchers from Texas A&M and Ohio State University, focusing on aerospace and medicine respectively. Additionally, case study 16 highlights how the outputs of university collaboration which utilizes strategic technology from abroad can result in potentially dual-use systems being developed by foreign nations. This is to say that even seemingly benign applications of strategic technologies can be used for military end uses once the university collaboration has completed. In this case study, an

[54] https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal
[55] https://www.cisa.gov/uscert/ncas/alerts/aa22-047a

encrypted communications network may be used for banking information, but is equally capable of transferring military information.

In the Russia context, there are examples of collaboration between foreign scientists and engineers with Russian scientists and engineers suspected of working on Russia's hypersonic glide vehicle projects. Joint papers and patents show links between key aerospace centers involved in weapons development and western actors.[56] Individuals from the United States and European countries who collaborated on topics such as combustion, fuel injection and other problems faced by vehicles travelling over Mach 5. It should be noted that most all collaborations occurred before 2014. Russia has leadership in this space given the resources and manpower dedicated to the problem, but foreign collaboration still allows scientists and engineers to exchange notes with foreign colleagues and potentially overcome bottlenecks. There is not necessarily anything wrong with academic cooperation with Russian nationals, but organizations, must be careful to vet whether or not the knowledge being used can be used to design, produce or manufacture weapons in the future

Acquisition Trends in the China-Specific Context

Attempts to acquire trade secrets and foreign expertise or technology are not uncommon to the PRC. While there are many methods by which many countries attempt to obtain export-controlled technologies, there are certain strategies the PRC employs that are notable trends. This section details technology acquisition methods by which the PRC has attempted to acquire said technology or expertise. The PRC, however, does not employ all these tactics equally in frequency or efficacy. Some methods of acquisition have even been outlined in their Five-Year Plans for science and technology. Namely, recruitment strategies such as the Thousand Talents Plan are emphasized as a method of bolstering their manufacturing base by relying on foreign human capital.

Strategic Entity Procurement and Tenders

Section reserved.

Investment and Acquisition Financing

As a direct method for the acquisition of foreign technology, investment and acquisition financing are not the primary tool used by the PRC. It is, however, worth noting that the Belt and Road Initiative being undertaken by the PRC does utilize financing schemes to gain leverage to set up infrastructure projects (namely around ports, but not exclusively) and create opportunities for Chinese businesses. While not necessarily problematic, as foreign direct investment is a routine practice states engage in, the end result in many of these BRI cases is an attempt to gain ownership of foreign

[56] CNS extracted data from Russian academic websites using Russian language keywords for hypersonic flight research. Non-aerospace related items were cleaned from the data with the remaining being analyzed by CNS.

infrastructure or investments.[57] Ports are the primary target in this scheme as they are part of the PRC's String-of-Pearls strategy for securing trade routes.[58]

Another way the PRC has utilized acquisition financing to attempt to obtain companies producing specialized components that they cannot yet indigenously produce. These types of acquisitions are typically blocked by national governments if they are in a strategic sector. One such example was the attempted acquisition of Arm, a British semiconductor firm, by the PRC in 2021 which was ultimately blocked by the British government.[59]

Joint Ventures

It is not uncommon for the PRC to enter into joint ventures with third party countries to develop certain technologies. This strategy can be employed either to jointly develop specific research or as a conduit for recruitment to Chinese companies or university positions to further research strategic topics for the Chinese government, such as in the case of the Texas professor with connections to NASA research (case study 4). The main consideration for companies entering joint ventures with the PRC is the control and protection of jointly developed intellectual property if it is strategic in nature. Joint ventures can also lend themselves to other economic or industrial espionage efforts undertaken by the PRC through cyber theft or recruitment of personnel even if it does not directly result in the transfer of intellectual property.[60]

Recruitment of personnel or students

Hand in hand with university collaboration is the strategic attempt to recruit expertise from foreign nations to supplement the labor required to expand strategic sectors in line with the PRC's national goals. The recruitment strategies of the PRC tend to prioritize those working at laboratories or in university settings, frequently targeting students as well as existing experts. This is not to say that recruitment of personnel within companies to steal technology or move to China with their expertise does not happen, just that many of the more systemic efforts are aimed at students or personnel in research institutes/labs actively developing new technologies.

---

[57] Berger, Blake and Russel, Daniel, "Weaponizing the Belt and Road Initiative" Asia Society Policy Institute, September 2020. https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf

[58] Thorne, Devin and Spevak, Ben," Harbored Ambitions," Center for Advanced Defense Studies, April 17, 2018.

[59] https://www.bloomberg.com/news/articles/2021-07-07/u-k-to-examine-chinese-takeover-of-biggest-u-k-chip-plant#xj4y7vzkg

[60] For example, the following case shows how an individual can be recruited for industrial espionage efforts and still not result in any IP transfer: https://www.justice.gov/opa/pr/chemist-sentenced-stealing-trade-secrets-economic-espionage-and-wire-fraud

The primary means of recruitment is the Thousand Talents Plan (TTP). The TTP leverages educational and employment opportunities in the PRC to attract foreign talent to work in China. Additionally, the TTP has been connected to instances of former TTP affiliates researching at universities outside of China with the goal of returning with information on strategic technology or to recruit additional members. CNS case studies 5, 4, and 6 highlight examples with researchers linked to the National Institute of Health, NASA, and the Cleveland Clinic, respectively.

Frequently the individuals who are operating in the US as part of the TTP could be identified with proper vetting controls for researchers in strategic fields. Occasionally these individuals leverage their foreign work for higher positions at the universities they return to in the PRC which may help in identifying the flow of strategic information if a TTP representative has been part of a strategic project in the US or another foreign country.

Outside of the TTP, there are other examples of individuals claiming they were recruited by a contact in the PRC to ship technology to the PRC for duplication, though these cases are less frequent. In this instance, case study 11, the woman that attempted to ship jet plane parts from Florida to the PRC referred to her contact as a 'technology spy'.[61]

University Collaboration – China-Specific Nuances

The importance of university collaboration in tech and knowledge transfer is especially true of the PRC wherein the university system in strategic fields work in tandem with the government institutions and private companies that are active in the same space. Within the PRC, there is a high level of coordination between government, industry, and universities. Due to a high level of state planning, there are pipelines from university into jobs for those being educated in strategic fields. Because of this, there are often geographical hubs within the PRC for specific strategic sectors where the top universities and corporations are in the same province or city. This can be helpful in guiding effective due diligence when considering whether to supply a foreign university with strategic technology.

Acquisition Trends in the Russia-Specific Context

Acquisition means of physical goods by Russia share many overlaps with those seen in the China context. Licit purchases, illicit procurement via front companies and misrepresentation are all common approaches. This section explains the acquisition trends specific to the Russia context and the unique patterns of how front companies and intermediaries are used in the Russia context given the extensive use of these means. Like in the China context, these means are not employed in equal frequency or efficiency. Rather, the use of these techniques will vary in professionalism and sophistication given the individuals and entities involved.

---

[61] https://www.justice.gov/opa/pr/california-woman-sentenced-50-months-prison-conspiring-illegally-export-fighter-jet-engines

Acquisition of Complete Item

In the Russia context, depending on the function of the purchaser or perceived sensitivity of the item, the entities may procure a completed item rather than components. For example, in Case Study 25 we see Military Unit 95006, who are accused of administering military bunkers in Moscow procured completed calibrators from the United States. In other cases, the line between production components and completed items can be blurry. This is best illustrated in Case Study 26, where the German Reflow ovens for manufacturing microelectronics was acquired as a complete unit. In this case the oven is procured as a single unit, but also serves production on sensitive items inside Russia. This is likewise relevant to Case Study 24, which involved procurement of completed production machinery by Russian defense entities.

Front Companies and Intermediaries – Russia Nuances

While not just a Russia phenomenon, the most common tactic employed to access restricted technology is to have another entity buy it for you. There is a more 'Classical' route often comprising a transfer to Finland and then via ferry or land border to Saint Petersburg. Case studies 20, 21 and 22 compiled by CNS all show this route remains workable despite its Cold War origins. In some schemes the proliferators will send the good to a country near Finland, such as Estonia, to raise fewer suspicions such as occurred in Case Study 22, the Flider Case. Once the items reach Russia, they can be distributed to buyers among the country's weapons manufacturers and intelligence agencies. Now the primary concerns are former Soviet republics in the Caucuses and Central Asia.[62]

The even simpler option is for a Russian company to directly buy the good from abroad and then sell it to the country's weapons manufacturers and intelligence agencies such as what occurred in the Novichok case.[63] The true extent of this is difficult to ascertain given the built-in plausible deniability of dual-use goods, but analysis of Russian customs records and procurement documents by CNS indicates a large nexus between third parties and Russian entities of concern.[64] This includes both defense contractors and Russia's security services. These intermediary companies are often listed as 'wholesalers' which while technically true, does not mean they are not also a defense sub-contractor. Whether or not a buyer is also a defense subcontractor can often be identified with a simple Google search of their name against Russia's relatively transparent contract bidding processes and a confirmation of the proper address.

---

[62] https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

[63] https://www.fontanka.ru/2021/03/05/69797849/

[64] CNS has conducted granular analysis of hundreds of transactions between third parties with access to Western supply chains and Russian entities of concern.

Sectoral Analysis

It is widely recognized that certain technologies, including emerging or foundational technologies, can be leveraged by Russia and China to substantially advance their military and strategic capabilities in a short time period. This is reflected in the national science and technology plans of both countries as detailed in other sections of this guidance. Given this, in preparation of this guidance, CNS undertook sectoral mapping for nine strategic technology sectors. Generally, the purpose of this sectoral mapping was to understand the global supply chain for these technologies particularly as it is relevant to strategic competition. In some cases, the sectoral mapping focused more on the status of Russia and/or China in relation to the sector. The table below lists the sectors examined.

Scope of Sectoral Analysis

Sector	Global	Russia	China
Carbon Fibre (scoped around PAN carbon fibre)	X		X
Aerospace (for Russia scoped around hypersonic missiles, for China scoped around aerospace and space systems)		X	X
Machine Tools (defined as having five or more axes)			
Semiconductor (scoped around or more axis)	X	Limited	X
Telecomms (scoped to include quantum communications, etc)		X	X
Biotechnology (scoped to include gene editing, etc)		X	X
Robotics (scoped to include autonomous systems)		X	
AI/Machine Learning (scoped to focus on inclusion in military and strategic systems)		X	X
High Performance Computing			X

In examining these technologies, the goal of this guidance is to identify what companies need to know and to safeguard their technology. Given this, each subsection concludes with a concise takeaway's section.

Artificial Intelligence

The term Artificial Intelligence – or machine learning – is a computer science technique in which models are trained to make predictions. Machine learning can be

used to make predictions about any subject provided that an appropriate library is fed appropriate training data. The libraries used to train models (i.e. Tensorflow) are open source and the hardware used for training algorithms is generic. Given this, while there are many ways in which machine learning can be misused, CNS has previously recommended that the focus of control should be on training data and the trained models where either of these has been developed in relation to specific military or weapons of mass destruction end uses.65 Some countries may go further in controlling these also in relation to human security considerations (i.e., facial recognition etc.). The potential elements to be controlled are thus as follows:

- The training data where the training dataset was designed to address a specific military or weapons of mass destruction related end use. For example, the identification of tanks from aerial reconnaissance.
- The trained model resulting from use of such training data. The model will typically be one or more computer files.

CNS has also observed that while many machine learning models can be deployed on generic computer hardware, for certain systems custom hardware is developed. For example, Tesla has designed its own hardware for running the model in Tesla cars.[66] For many military deployments of AI, it is perhaps likely that custom hardware would also be designed. For example, this could be the case on a military aircraft where the hardware must be designed to meet the operating and environmental considerations associated with the aircraft. As such, it is recommended that hardware specifically designed for running machine learning algorithms in military systems be subject to control.

In a PRC context, AI applications are applied in conjunction with a many other fields. Namely, the Five-Year Plans mention the integration of AI into manufacturing processes and other sectors to 'intelligize' the economy.[67] For this reason, it is important to consider how to secure AI's applications as well as the algorithms and hardware themselves. Outside of integrating AI into manufacturing methods, AI has been used by the PRC in security and surveillance both domestically and abroad. The PRC has an initiative to develop and deploy 'smart cities' which integrate AI into the infrastructure of the city and incorporates systems such as automated ticketing for jaywalking. Many of these smart cities are being developed along the Belt and Road Initiative and in countries partnered to the program. The technology is being developed

---

65 https://nonproliferation.org/export-control-and-emerging-technology-control-in-an-era-of-strategic-competition/

66 https://www.wired.com/story/why-tesla-designing-chips-train-self-driving-tech/

67 English Translation of "Proposal of the Central Committee of the Chinese Communist Party on Drawing Up the 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2030" https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf

by ZTE or Huawei.[68] While seemingly benign, these systems, especially when deployed in foreign countries, collect large amounts of data on the movements of citizens and for the fine-tuning of facial recognition AI. This data can be used to police domestic citizens or target foreign citizens.

The PRC has also shown that they can employ AI for targeted schemes to steal information from foreign companies, such as the examples in case studies 3 and 8 where hacking groups used AI to gain access to company networks and potentially digital information for strategic goods. This is in line with research on PLA contracts on AI which showcase how the PLA is prioritizing AI advancements in information and electronic warfare. However, this is overshadowed by their focus on intelligent and autonomous vehicles.[69]

China's most clear shortcoming in machine learning is the production of specialized hardware. However, not all applications of AI require specialized hardware. The capacity to develop and produce such hardware is tied to the state of China's semiconductor and supercomputer industry, covered in their own sections below in more detail.

Russia has put together a national strategy for the development of artificial intelligence. The strategy plans to increase the country's expertise in machine learning, create machine learning focused education programs, datasets, infrastructure and reforms of the legal architecture to greater facilitate the growth of the space.[70] The Russian government hopes to make use of the country's strong cadre of scientists and engineers to make Russia a player in the AI space. Russian companies such as Yandex are competitive globally in certain AI applications such as image recognition and self-driving vehicles with a presence on international markets given the company's relatively early embrace of the technology.[71] It remains to be seen how Yandex maintains this foothold in the post-24th of February reality.

The Russian military openly discusses its ambitions for introducing machine learning into weapons systems. Specifically, there is a body on research and discourse on applying computer vision, or complex object identification into military systems.[72] The Russian military, known for its infamous micromanagement and distrusting of its own soldiers, see the targeting and identification applications for precision weapons as a

---

[68] https://e.huawei.com/en/services/industry-consulting-and-application-integration/smart-city#:~:text=Huawei%20provides%20a%20comprehensive%20Smart,talent%20development%2C%20and%20project%20management.

[69] https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf

[70]

[71] https://voicebot.ai/2019/05/17/local-knowledge-and-personality-help-yandexs-alice-virtual-assistant-dominate-the-russian-market/

[72] https://web.archive.org/web/20211027050021/https://iz.ru/800451/aleksei-kozachenko-aleksei-ramm/zashchitnyi-kontur-vvs-i-pvo-kryma-obedinil-iskusstvennyi-intellekt

boon. The Russian military claims that it has already built machine learning into parts of its air defense system for Crimea.[73] Other applications that have both civilian and military potentials discussed by Russian researchers are on ways machine learning can optimize flight paths and the general efficiency of UAVs.[74]

Takeaways

Russia and China are both working to integrate machine learning into strategic and military systems. To do this, both countries are likely to leverage open-source software and data. They are also likely to seek proprietary models and training data including by leveraging their powerful cyber warfare capabilities. These countries may also seek to use cloud services to train their machine learning models (see the High-Performance Computing section below). Given this, entities that develop models and training data that could be used for military and strategic systems should safeguard the data including by adhering to best cybersecurity practices. Such proprietary data should not be posted openly on the internet without careful consideration, and authorities should be consulted on whether the posting of such data could constitute an export of technology as defined by national export controls.

High-Performance Computing

This section focuses on various forms of high-performance computing, not just high-performance computers (HPC) as a traditional supercomputer. The intent is to capture the quantum computing and cloud computing sectors which have unique applications and nuanced advancements relative to supercomputers.

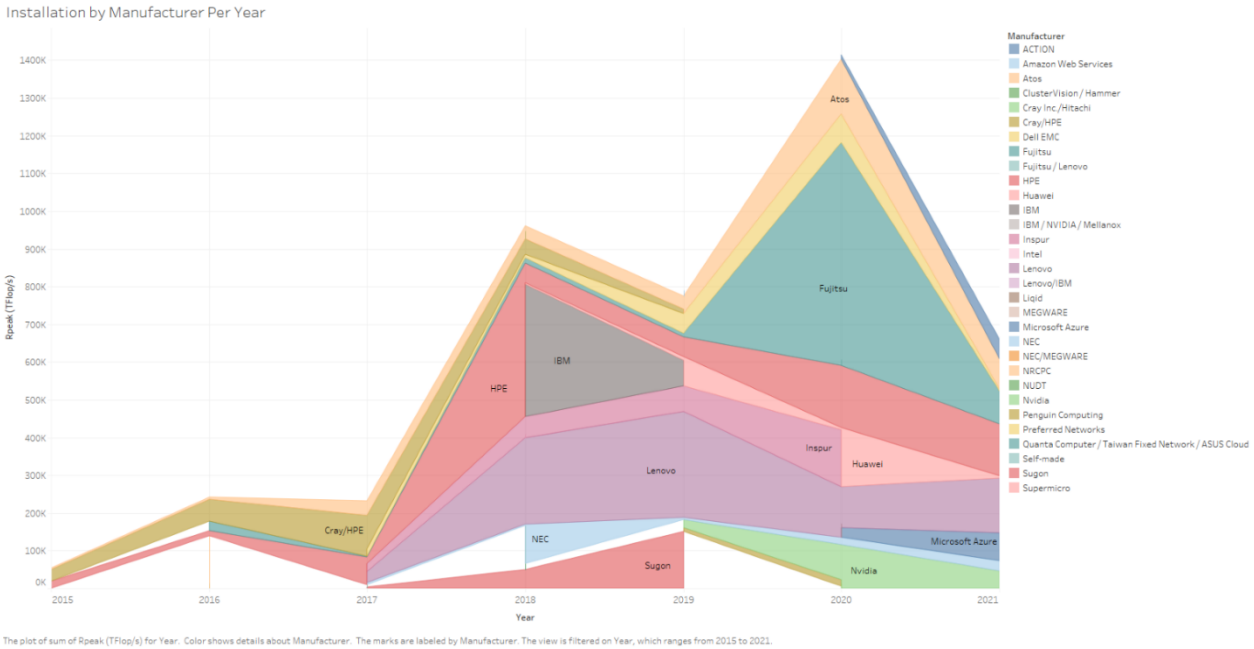
High performance computers – or supercomputers – are generally carefully designed and connected standard computers. Supercomputers can use either CPU or GPU cores – versions of which can be found in every PC or laptop. Large numbers of either or both of these are interconnected to achieve the required performance characteristics. There is thus nothing particularly unique in the processing hardware of super computers. Because of this, the global leaders in supercomputing are also those who lead in commercial components for PCs, such as NVIDIA, Fujitsu, IBM, and Huawei. There is a running 'top 500' list[75] that tracks the most technically powerful supercomputers; however, this does not necessarily mean that they have the most useful applications. Factors that do not relate directly to the processor hardware such as network latency,

[73] https://web.archive.org/web/20211028205257/http://pstmprint.ru/2017/03/14/%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F-%D1%81%D1%82%D0%B0%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C-%E2%84%96-1-2017/

[74] https://research.sfu-kras.ru/publications/publication/46536174

[75] https://www.top500.org/

energy use and cooling are among the main considerations that must be taken into account. The figure below maps the top manufacturers of supercomputers globally based on the TOP500 dataset.



In this context, there are two principal modalities through which a supercomputer transfer could occur. First, a large number of CPUs or GPUs or a type suited for use in a supercomputer could be acquired by an actor in a country of concern. Second, a company could be contracted to design and build a supercomputer. The provision of either of these services should be controlled such that scrutiny can take place of the entities and end uses to which the supercomputer will be put. A third pathway is the provision of cloud-based computing services as examined below.

Within the PRC, as with many other sectors, there are a few primary companies with a variety of subsidiaries that perform more specific research or production functions. The organization of industry also synergizes with the network of National Supercomputing Centers which house the computers and utilize them for research. The two main centers of strategic interest are the ones in Wuxi and Guangzhou which house a SunwayTaihuLight and Tianhe-2A supercomputer respectively. Sunway is the leading producer of supercomputers domestically in the PRC and the Sunway TaihuLight was the 6th most powerful supercomputer in the world at the time of writing this report with 93 petaflops. What makes this computer impressive is that the PRC claims this computer is built with solely domestically produced processors designed by Shanghai High Performance IC Design Center. This chip, the Sunway SW26010 is manufactured

using the SMIC 28nm node.[76] While the limitations of the PRC's semiconductor production is covered in another section, HPC specifically requires an interconnect technology that allows for the various CPUs to function in tandem. NVIDIA leads globally for this processor interconnect technology, at least for GPUs, and it is a chokepoint limitation on the PRC's ability to indigenously produce full HPCs at the highest levels.

Quantum computing is an emerging technology with limited commercial applications but potential applications for both strategic and civil sectors. Quantum computers are quite different from regular computers, using entirely different types of hardware that work on different physics principles. Quantum computers work on the basis of quantum bits or 'qubits' instead of the traditional ones and zeros for classical computing. The most common form of qubit is a superconducting qubit which are already used in a variety of quantum computers and were first used in prototype computers by IBM and Google. Global leaders in the quantum space are thus likely to be producers of traditional supercomputers. However, due to this being an emerging technology, the start-up space in quantum is fairly active. Thus, countries with the leading producers are the United States, the PRC, Canada, and the UK. It is important to note that many of the start-ups are only in the research and development stage and have yet to produce any commercial products. This can make tracking and managing all active entities in this strategic space quite difficult because nothing is being exported or imported. These factors do however place an important emphasis on the recruitment of personnel and the management of expertise on quantum technology and engineering.

In the PRC specifically, there is a strong connection in the quantum sector between government, universities, and commercial institutions. Because the space is fairly small with a niche and relatively new education required, university collaboration[77] is a common method of technology acquisition. Like in the US where large tech giants like IBM have a quantum division, major Chinese firms like Baidu, Huawei[78], and ZTE have quantum relevant divisions. That said, it is important to draw a distinction between quantum computing and quantum communications. While quantum computers are required to facilitate quantum communication, this section focuses on the hardware of the computers while the telecommunications section includes quantum communications.

Due to quantum computing being such a specialized field, the PRC has consolidated a lot of resources in the Anhui Province, namely in Hefei and Wuhu City.[79] The exception to this is the quantum departments of the larger companies that do not inherently

---

[76] https://www.linleygroup.com/newsletters/newsletter_detail.php?num=6285&year=2021&tag=3

[77] http://www.originqc.com.cn/en/website/companyProfile.html

[78] https://cloud.huawei.com/

[79] This is informed by CNS mapping work for quantum computing.

specialize in quantum, like Baidu[80] and Huawei which may have their quantum headquarters in Beijing or Shanghai. This hub in Anhui houses multiple businesses and universities that have quantum departments. The USTC's Division of Quantum Physics and Quantum Information in Hefei[81] is the premier research center in the PRC on quantum technology and actively recruits students and personnel that work on projects with national labs and companies in the area and can serve as a diversion risk for quantum technology and data. One company that exemplifies these connections is QuantumCTek in Hefei.[82] This start-up was founded by researchers at USTC and recruited students from the program for work. QuantumCTek developed the dual-use quantum encryption technology referenced in case study 16.

The PRC's shortcomings in the ability to produce sub 10nm microchips, covered in the semiconductor section, also implicate quantum technology development and scalability. That said, as the PRC is advancing its indigenous semiconductor manufacturing capabilities, two of China's tech giants have advanced quantum computing systems in tandem. In 2022, Baidu[83] released its first quantum computer and Huawei applied for a patent for a quantum computer and chip.[84] Since most applications are still theoretical, however, it hasn't had an immediate impact on their ability to progress research in other areas. The PRC is not necessarily behind on the application of quantum technology relative to other states, but key challenges like cooling will be a limitation on all industry participants. Due diligence efforts should thus focus on controlling access to expertise and equipment, especially with relation to specific geographies in the PRC.

Cloud computing in the PRC is organized in a similar way with start ups being fairly common but larger companies, namely Alibaba, leading the pack domestically. One of the primary strategic uses of cloud computing is in supercomputing or quantum computing as a service. This is where a cloud provider would facilitate the opportunity for an organization to run programs on their hardware without the need to obtain the hardware themselves. This creates a unique control risk because it allows organizations to potentially benefit from controlled hardware while anywhere else in the world and without a need to obtain a license. Cloud service providers should thus consider due diligence on organizations buying cloud services and the locations of said organization, especially when running potentially strategic simulations or programs.

The most prominent cloud service providers are based in the United States, such as Microsoft, Amazon Web Services (AWS), and Google. The PRC does have a domestic

---

[80] http://research.baidu.com/
[81] https://quantum.ustc.edu.cn/web/en
[82] http://www.quantum-info.com/English/
[83] https://www.reuters.com/technology/chinas-baidu-reveals-its-first-quantum-computer-called-qianshi-2022-08-25/
[84] https://thequantuminsider.com/2022/06/20/huawei-files-patent-for-quantum-chip-computer/

competitor to these companies in Alibaba. Alibaba Cloud offers an Elastic GPU Service to facilitate deep learning, video processing, scientific computing, and visualization.[85] These services use the following GPUs: AMD FirePro S7150, NVIDIA Tesla M40, NVIDIA Tesla P100, NVIDIA Tesla P4, and NVIDIA Tesla V100, which are components of American origin. This highlights a reliance on foreign components to be competitive in this space. Thus, due diligence for cloud computing must also include effective due diligence by hardware producers. Cloud service provision of supercomputing capabilities offers a path to shortcut the challenges and cost associated with acquiring supercomputer hardware. Given this, efforts are needed to ensure cloud service providers are compliant with relevant laws and to ensure western hardware is only supplied to cloud service providers who adhere to compliance standards equivalent to those in the west.

Takeaways

Given these factors, Russia and China are likely to be reliant on the international marketplace for high performance computing capability in the years ahead, albeit in different ways. Russia's lack of production capability and challenges in sourcing modern computer hardware will mean that Russia will be reliant on previous generations of technology for its military and strategic purposes. Russia is likely to continue to seek computer equipment and components illicitly and from the secondhand market. Russia is likely to seek manufacturing equipment and know-how including high performance computing consultants and computer and component design experts (see also the semiconductor sector).

China possesses and is likely to be able to continue to acquire advanced computing capabilities including supercomputers. Principally, these technologies are assembled using foreign source materials and components as China's semiconductor industry (see below) is not yet competitive with the international marketplace. Given this, the focus for China should be in ensuring that any high-performance computers or components thereof supplied to China are not acquired by military and strategic linked entities. This, in particular, is likely to be challenging given the close integration of many Chinese universities with China's strategic programs through its Military Civil Fusion program. Companies should undertake careful due diligence and ensure they know the true end user when exporting specialist software, hardware, datasets, or models to China. Particularly where transactions involve defense, aerospace, space or another strategic sector, companies should consider referring all cases to national authorities for review. Cloud service providers should also ensure that they do not make services available to military end users in China. Western hardware providers should take steps to ensure

[85] https://www.alibabacloud.com/product/computing?spm=a3c0i.239195.6791778070.134.192012bdUWtkFy

any cloud service provider they supply in China is equally implementing compliance approaches.

Semiconductors

Semiconductors in the context of integrated circuits and microelectronics are electronic devices that power and enable everything from televisions sets to cars and computers. Semiconductors are critical for the creation and functioning of various defense modernization efforts and emerging technologies with defense applications.[86] As such, the United States and other states have prioritized both domestic production of these items and acted to secure their own supply lines to these critical devices. Broadly, the design and manufacturing of cutting-edge semiconductors is structured in such a way that designers of cutting-edge integrated circuits, sometimes referred to as chips, outnumber the number of manufacturers of cutting-edge integrated circuits. Taiwan-based TSMC is a leading manufacturer of cutting devices and center for much of the semiconductor discourse.[87] Various designers, such as Intel and other leading semiconductor companies contract the actual building of devices to TSMC and other fabrication plants.

China likely does not have the capability to produce small feature size (sub 10nm) semiconductors at commercial scale. While there are a number of barriers to this, one main barrier is the need for precision specialist production equipment which is only manufactured by one company – ASML in the Netherlands. In the absence of this, Chinese entities also outsource production of sub 10 nm products to the only companies with semiconductor fabs capable of manufacturing such devices: TSMC and Samsung.

That said, China does have mainland producers of semiconductors as indigenous integrated circuit technology is a top priority of the Five-Year Plans. The largest foundry in the PRC is Semiconductor Manufacturing International Corporation (SMIC) which has processes ranging between 14 nm and 0.35 micron.[88] In December 2020 SMIC announced a new venture, SMIC Beijing which would increase the number of 12-inch wafers per month. That same month the U.S. Bureau of Industry and Security (BIS) added SMIC to the Entity List due to its relationship with the PRC military.[89] SMIC joined dozens of other semiconductor related entities to be restricted in recent years. While

---

[86] https://www.csis.org/analysis/semiconductors-and-modern-defense-spending

[87] https://thediplomat.com/2021/11/how-taiwan-underwrites-the-us-defense-industrial-complex/

[88] "Foundry Solutions," SMIC, accessed February 27, 2021, https://www.smics.com/en/site/solution.

[89] "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List," Federal Register, December 22, 2020, https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities#:~:text=This%20rule%20adds%20SMIC%20and,)%20Co.%2C%20Ltd.%3B.

this may slow down slightly the rate of innovation in this field by the PRC, there is also a risk to US market share when restrictions are only applied unilaterally. While these restrictions prevent US companies from engaging with the inevitable Chinese semiconductor market, it may be ceding that market share to competitors in countries like South Korea or Japan. This has also, in turn, largely decoupled the semiconductor industry in China from the US which limits various forms of market-based leverage. Most recently, in 2022 TechInsights reported that 7nm SMIC technology was found in bitcoin mining technology and represents a leap in indigenous production by the PRC, despite sanctions.[90] In the follow up report by TechInsights released in August, analysts concluded that the SMIC technology had advanced to levels that can rival Intel, TSMC, and Samsung. In the report, many comparisons are made between SMIC's design and that of TSMC. [91]

Outside of specific fabrication limitations, design information and know-how is one area the PRC lacks. However, joint ventures have served as a means for the PRC to access such technology. Namely, China acquired the British firm Imagination Technologies and has a joint venture with ARM in Japan to cover many of these gaps. According to some studies, 95% off Chinese chips incorporated IP licensed from ARM.[92]

Russia has striven to upgrade its capacity to build a domestic alternative to foreign semiconductors vital to the functioning of a modern society. Before TSMC ceased cooperation with Russia had been partially successful in less advanced semiconductor manufacture and could [93] produce up to 28nm chips with cooperation of outside fabs. i.e. the devices are designed in Russia and were manufactured in Taiwan.[94] That is no longer possible with the current trade restrictions. One of the more advanced of these Russian designed chips, the Elbrus 16s CPU however, is still behind the latest CPUs designed by Intel or AMD. The Elbrus and Baikal processors were produced by TMSC and are used in Russia's military, intelligence and government systems as replacements for Western semiconductor devices which their military, intelligence and government systems are currently reliant on.⊠ Reliable Russian media reports indicate

---

[90] https://www.techinsights.com/blog/disruptive-technology-7nm-smic-minerva-bitcoin-miner

[91] https://www.techinsights.com/blog/smic-7nm-truly-7nm-technology-how-it-compares-tsmc-7nm

[92] Khan, Saif M., Alexander Mann, and Dahlia Peterson. "The Semiconductor Supply Chain: Assessing National Competitiveness." Washington, DC: Center for Security and Emerging Technology (2021).
APAC Equity Research Reports - Credit Suisse, Global Semiconductors Sector, The uneven rise of China's IC industry, January 20, 2021.

[93] https://www.kommersant.ru/doc/5230512

[94] https://www.kommersant.ru/doc/5129386

that many of these chips [95]have poor quality control and are [96]▣ Russian semiconductor producers are discussing moving to the Russian chip manufacturer Mikron (not to be confused with the U.S.-headquartered Micron), whose manufacturing capability of 65nm means Russia will be domestically producing slower, less powerful chips in the near future.▣ [97]mid 2000s, meaning that Russia's indigenous semiconductor manufacturing capability lags around two decades behind the global marketplace.[98]

In August 2022, the US began implementing the CHIPS and Science Act which is aimed at increasing domestic production capacity of advanced microchips. In addition to the act itself being signed into law, President Biden has signed an executive order to jumpstart the effects of the legislation by investing in American chip producers and chip research.[99] This law does have direct implications for industry and the military as reliance on a foreign chip producer can undermine military readiness.[100] Lastly, the US reportedly implemented additional new restrictions on Nvidia and AMD which would bar sales to Russia and China of high-end chips.[101] This includes Nvidia's A100 and H100 integrated circuits. AMD reported that they have been ordered to stop selling the MI250 chip used in high performance computers. Interestingly, they are not barred from selling the MI100 chip to China. While these measures were not formally announced by US officials, a spokesperson was quoted saying that more measures are likely underway to curb MCF programs in China.[102]

Take Aways

It is a strategic priority for China to indigenize production of small feature size semiconductors and, in the interim, to acquire semiconductor devices from the international marketplace. China will seek semiconductor manufacturing equipment including lithography designed for the Extreme Ultraviolet Wavelengths and associated manufacturing equipment and chemicals. China will also continue to seek to recruit individuals and send staff overseas to acquire semiconductor manufacture know-how. Companies should consult with their national authorities concerning approaches for any of these. China will also seek to acquire high end semiconductors including by 1) outsourcing production to any of the fab as a service semiconductor manufacturers such as TSMC in Taiwan; 2) by acquiring specialist devices from companies who

[95] https://www.kommersant.ru/doc/5192750

[96] CNS research and https://www.rbc.ru/technology_and_media/30/05/2022/6290e5e39a794746a563548c and https://www.airvers.com/the-russian-semiconductor-industry-worsens-after-giants-joined-the-sanctions-team/

[98] https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_65nm

[99] https://www.cnn.com/2022/08/25/politics/chip-manufacturing-biden-executive-order/index.html

[100] https://foreignpolicy.com/2022/08/26/chips-act-us-china-semiconductor-tech-taiwan/

[101] https://fortune.com/2022/09/01/nvidia-amd-chip-sales-ai-china-russia-military/

[102] https://www.nytimes.com/2022/08/31/technology/gpu-chips-china-russia.html

produce them (i.e. by companies who could themselves use semiconductor fabs), and 3) through distributors of manufactured devices. Companies should undertake due diligence on any approaches in these categories with the goal of ensuring that the Chinese entities involved are not linked to military or strategic programs and will not use the devices for military or strategic ends. Companies should work closely with their national authorities to this end.

The Russia case is somewhat more straightforward. As a result of Russia's invasion of Ukraine, most countries have decided to restrict or prohibit the export of semiconductors and semiconductor manufacturing equipment to Russia. Given this, any approach from a Russian entity should be referred to national export control authorities. Russia can be expected to seek to evade the semiconductor restrictions including by attempting to acquire goods through third countries including in Russia's near abroad. Given this, companies should undertake due diligence particularly to ensure that transactions are not destined for Russia. Companies should also avoid using untrusted distributors in Russia's near abroad.

Aerospace and Space

Aerospace covers a broad range of technologies covering everything from civilian aircraft to missiles and satellites. This broad range of devices includes engines, composite materials, and emerging capabilities such as hypersonic glide vehicles developed by Russia and China and being developed by the United States. Engines, composite materials and hypersonic glide vehicles each have their own technical and engineering nuances, being areas of expertise unto their own.

The aerospace and space sectors in China and Russia pose particular trade compliance challenges. In the case of China, there is little to no separation between the entities involved in the military program and the civil space program. When dealing with China, countries should ensure they have adequate mechanisms in place to review all cooperation with space-related entities. This could include an expressed callout in the military catchall or publication of a list of Chinese space-related entities.

While most Chinese aerospace entities have a specific focus, whether in the civilian sector or military sector expressly, these companies are generally just subsidiaries of two or three aerospace 'giants' which actively utilize MCF practices. For these reasons, due diligence in commercial aerospace is critical to the security of western technology. The exemplary case for MCF in the aerospace context was the testing of a hypersonic glide vehicle capable of circling the globe in 2021.[103] While foreign reports on the test indicate that the vehicle is capable of being weaponized, the PRC insisted that this

[103] https://www.armscontrol.org/act/2021-11/news/china-tested-hypersonic-capability-us-says

technology was in a civilian program.[104] Due to the organizing structure of the aerospace industry in the PRC, however, it is likely that the vehicle was a subsidiary of a company with connections to the military.

In more expressly military settings, the PRC has a network of research institutions that work directly with the commercial producers of said technologies. This is not inherently dissimilar to how companies like Raytheon and Lockheed Martin work in the US. However, there are fewer barriers between civilian and military research activities. The result is major producers such as the Aviation Industry Corporation of China (AVIC), China Aerospace Science and Industry Corporation (CASIC), and Commercial Aircraft Corporation of China (COMAC) all having highly specialized subsidiary companies with explicit goals. So, while one subsidiary may be working in commercial spaces, there will be another subsidiary focusing on military applications, and so forth. For example, since COMAC produces commercial aircraft and AVIC military (and commercial) aircraft, each would have a similar subsidiary that focuses on the production of heavy machinery.[105]

Ultimately, the PRC is fairly self-sufficient in the ability to manufacture advanced aerospace systems, however, the PRC does lag in aeroengine development and is still reliant on foreign imports for some key components. To address this gap, AVIC and COMAC have jointly started Aviation Engine Corp General Information (AECC) to develop aeroengines.[106] Detailed further in sections below, and in case studies 3, 8, 10, and 15, there have been many instances in the last decade in which the PRC attempted to illegally obtain aeroengine research or equipment from abroad. The PRC works closely with universities, research institutes, and foreign partners to facilitate the acquisition of foreign technology.

A particularly important aspect of the China challenge for aerospace concerns the interconnection between its space programs and missile programs, with the same entity, the China Academy of Launch Vehicle Technology, being responsible for both. CALT is part of the larger China Aerospace Science and Technology Corporation and many other CASC subsidiaries are also involved in both military and civil space programs. Given this, ensuring that cooperation and technology supply is for civil purposes only can be challenging meaning that companies should consider referring any such cases to their national authorities for review.

Russia is arguably a global leader in advanced aerospace technologies such as hypersonic glide vehicles and related technologies. The area has the firm support and backing of state leadership. Russia uses a strong and longstanding network of military

---

[104] https://www.cnn.com/2021/10/18/china/china-hypersonic-missile-spacecraft-intl/index.html

[105] CNS mapping efforts identified dozens of subsidiaries for each of these companies with niche supply chain roles to support each main company's efforts.

[106] https://archive.ph/I9Zh9#selection-4127.76-4127.137

research labs, universities and veteran scientists who have been working on the topic for decades to achieve their success in this sector. Russia historically has engaged in academic collaboration on the subject, including with Western defense firms and scientists close to NASA, but this collaboration declined after the 2014 annexation of Crimea and subsequent growing isolation.[107]

Given the scope of Russia's military aerospace and its level of importance to Russian national security it is impossible to predict the course of Russia's increased isolation on their military aerospace programs. Russia is relatively self-sufficient with a robust and well-funded infrastructure for the research, development and production of military aerospace projects. There are hundreds of entities in Russia from technical universities connected to the defense base, military research centers, testing facilities and repair plants dedicated to maintaining Russia's aerospace capabilities. [108] Russia is having problems with civilian engines post-February 24th, but the aerospace procurement information for military jets and secret research projects is classified and the extent of problems currently in that sector are unclear.[109] Russia has historically had problems with engine manufacture, but is still validating domestically produced military helicopter engines with potential Asian buyers.[110] Russia's ability to maintain and manufacture will ultimately be impacted by factors such as the ability to maintain the advanced machine tools of foreign origin required for their timely manufacture. As machines bought in the 2000s age and break down, more production bottlenecks will appear. [111]

Take Aways

Aerospace is one of the sectors with the least clear military/civilian distinction due to the inherent dual use nature of many aircraft components, the use of satellites by both militaries and civilian enterprises, and the fact that many of the same entities are engaged in both activities. This blurred line magnifies the need for effective due diligence beyond normal controls to identify where an entity may be engaged in military-linked activities.

Outside of the dual use nature of the sector, specific advancements in hypersonic technology, including hypersonic glide vehicles, are a priority area for both Russia and China. China, in particular, coordinates a number of aerospace related research and development efforts with its university system and national labs. As such, scrutiny of

[107] For this particular research CNS conducted keyword searches in Russian academic repositories for keywords related to aerospace and hypersonic flight to map connections between scientists at key aerospace research centers in Russia and foreign partners.
[108] List of Russian milititary aerospace centers compiled by CNS
[109] https://ridl.io/russian-civil-aircraft-manufacturing-in-2030/
[110] https://soyuzmash.ru/news/companies-news/sertifikat-tipa-dvigatelya-vk-2500ps-03-validirovan-v-yuzhnoy-koree/
[111] https://ridl.io/sanctions-and-the-russian-defence-industry/

transactions involving such entities, even in adjacent engineering focuses, is warranted.

Additionally, China's civil and space missile program are not separated with one entity, the Chinese Academy of Launch Vehicle technology, which itself is a subsidiary of China Aerospace Science and Technology Corporation, playing a key role in both programs. Given this, careful due diligence should be undertaken regarding any technology transfers to China's space sector particularly if it relates to these entities. In practice, this might mean referring all such cases to national authorities for review.

Composites

Carbon fiber is a specific composite technology that is a lightweight filamentary material. Currently, there are fewer than 20 prominent producers of carbon fiber globally with the leading producer being Toray Industries in Japan.[112] Europe and the United States also have various smaller producers of carbon fiber. As a material, carbon fiber has a number of properties that make it viable for both civil and military end uses. These properties include corrosion resistance, which is useful in uranium enrichment applications, and ability to sustain uniform tension, making it popular for a variety of aerospace applications, just to name a few.

China, in particular, has been working to indigenize carbon fiber production but has struggled as a result of technology, expertise and material challenges. China's lack of indigenous capability to produce the highest grades of carbon fibre is a key chokepoint for the country's military advancement. As a result, countries should consider carefully whether to export carbon fiber production equipment to China where the equipment would raise the country's capability to develop higher performance carbon fiber. Additionally, countries should examine what steps can be taken to control the provision of expertise and know-how to these production facilities (i.e., China's efforts to recruit foreign staff to run carbon fiber production facilities).

While efforts have been made in an attempt to acquire foreign expertise in carbon fiber production, the PRC still lags behind in both volume and mechanical property off the produced carbon fiber. While this does give them the flexibility to use indigenously produced carbon fiber for some applications, carbon fiber with advanced properties still remains a chokepoint technology because of its applications to a variety of the PRC's strategic sectors.

As of September 1, 2022, the Chinese entity Zhongfu Shenying announced they have produced indigenously the T-1000 carbon fiber for aircraft and missiles.[113] According to the company, the carbon fiber material is of the same level as the T-1000 from the

[112] This is based on internal CNS research which sought to identify all commercial producers of pan-based carbon fiber.
[113] https://inf.news/en/military/13e0f7fd30ae10f5fc9a36cff83e5adb.html

Toray Corporation of Japan. If truly indigenously produced, this would be a significant breakthrough for the PRC and could result in other indigenous capabilities in aerospace and space sectors. Specifically, the J-20 Chinese fighter jet could have a next generation with stronger carbon fiber.[114] The designation of T-1000 is a reference to carbon fiber applications prioritizing tensile strength and tensile modulus with main applications in aircraft bodies, missiles, and other vehicles. By contrast, an M-series carbon fiber is utilized for applications in spacecraft.

Take Aways

Both Russia and China are reliant on the international marketplace for composite materials, albeit to different extents. Russia lacks the ability to produce high end PAN-based carbon fiber, production equipment, and equipment to use it in applications, such as winding machines. China similarly lacks these, although Chinese companies claim to be able to manufacture modest quantities of industrial-grade PAN carbon fiber. Both countries are likely to seek carbon fiber from the international marketplace for use in their strategic programs. This includes efforts to acquire it from distributors. China is particularly focused on indigenization of carbon fiber production and is likely to seek production equipment and expertise from abroad. Such cases should be referred to national licensing authorities.

Biotechnology and Chemistry

Biology is an old science that has been around for a majority of civilized history. Despite the length of time spend in studying this science, major discoveries are made only within a little more than the past century. More recently, biotechnology have emerged to leverage this old science for many beneficial applications. From enhancing healthcare to increasing food security, biotech products have a significant impact on modern life. However, the risk of a bioweapon made possible by this emerging biotech also looms in the background. The biotech domain is undergoing substantial evolution at present, but emerging technology presents potential new threats, which will carry many implications for export controls. Additionally, these new biotechnologies are the result of integrating biology and other sciences, which introduces a variety of vulnerabilities. Cyber and sensitive information security are among the top concerns. CNS work to map out the biotech industries in countries of interest and gauge their risks and potential impacts on the international community. CNS have also reported on a supply chain network for Russian chemical weapon. While most traded chemicals have legitimate industrial uses, some are vital for chemical weapon production and can be diverted for this purpose. Additionally, chemical reagents are an important component to a majority of biotechnologies, thus warranting a collective analysis of both industries.

[114] Ibid.

China's chemical and biological contract development and manufacturing organization (CDMO) sector is an area of potential concern in its biotech industry. CDMO allows many researchers and biotech companies with limited resources and expertise access to these so that they may advance their objectives. Because of this accessibility, CDMO have the potential to lower barriers for chemical and biological development, thus providing actors that lack the resource and expertise to development these weapons of mass destruction an entry point.[115] A concern more prominent than non-state actors gaining access to developing chemical and biological weapons is that the Chinese government will have access to these CDMO for weapons development. Thanks to their Civil-Military Fusion policy, the PRC have access to the same barrier-lowering resources and expertise as well as any data resulting from partnerships with foreign entities. These datasets can be crucial for not only weapons development but also biotechnology advancement. The PRC have already leveraged their biotech industry to gather these data for questionable goals. They have collected genomic data from their Muslim minority, the Uyghurs, to development surveillance technologies tailored toward the population,[116] and from prenatal tests popular globally.[117] The same company collecting this genomic data, Beijing Genomic Institution (BGI) Group, have also been aggressively marketing their products to the West, including several states in the US, to use their genetic collection products as a countermeasure to the COVID-19 pandemic.

Other than China's CDMO service industry, its pharmaceutical industry also has a prominent presence in the global biotech market. Aside from medical products, China is one of the world's largest exporters of active pharmaceutical ingredients (API) and its API imports pale in comparison. While the biggest importers of China's APIs are geographically close to the country, such as Japan, India, and Vietnam, its global presence reaches almost all the other continents. Major countries on continents other than Asia include the United States, Brazil, Nigeria, and Germany. With the CDMO service industry and China's strong global presence as a major source of APIs, China has made itself one of the top destinations for global biotech development and research.

---

[115] Julie A. Carrera, Andrew J. Castiglioni, and Peter M. Heine, "Chemical and Biological Contract Manufacturing Services: Potential Proliferation Concerns and Impacts on Strategic Trade Controls," US DOE Office of Scientific and Technical Information, 1 April 2017. Available online at: https://www.osti.gov/pages/biblio/1390807-chemical-biological-contract-manufacturing-services-potential-proliferation-concerns-impacts-strategic-trade-controls (Accessed 13 July 2022)

[116] Sui-Lee Wee and Paul Mozur, "China Uses DNA to Map Faces, With Help From the West," The New York Times, 22 October 2019. Available online at: https://www.nytimes.com/2019/12/03/business/china-dna-uighurs-xinjiang.html (Accessed 13 July 2022)

[117] Kristy Needham and Clare Baldwin, "China's gene giant harvests data from millions of women," Reuters, 7 July 2021. Available online at: https://www.reuters.com/investigates/special-report/health-china-bgi-dna/ (Accessed 13 July 2022)

The biotechnology sector in Russia revolved around their agricultural biotech industry to ensure food security for its populace. While the country's biotech industry development was stagnant in the years following the collapse of the Soviet Union, a few in Russia's leadership recognized the sector's importance for national prestige and growth since the beginning of the 21st century.[118] Food security, a historically significant issue, was the main priority for development within the biotech industry. This led Russia to become one of the world's largest providers of wheat[119] and other agricultural products, even though their agricultural biotech sector relied on imported goods.[120] Many of these imported goods are to support the agricultural industries and include items such as livestock feed and seeds, totaling $16.3 billion from 2011 to 2020. Paraguay and Brazil are the top two countries that Russia imports its agricultural products from, totaling to $2.85 billion and $2.65 billion respectively. Germany ($1.42bn), Netherlands ($1.33bn), and China ($1.20bn) are the next largest source of agriculture produces for Russia. In comparison, Russia was able to export $21.5 billion worth of agricultural products, with its largest buyers being Turkey and China, at $6.6 billion and $2.5 billion respectively. China is a significant agricultural partner for Russia, in terms of imports and exports.[121]

Russia's pharmaceutical industry is another major sector for its biotech industry.[122] However, Russia does not manufacture enough pharmaceutical products to support its population, so the majority of the product is imported from other countries,[123] similarly to its agricultural sector. This reliance on imports extends to the raw materials used to manufacture pharmaceutical products, including active pharmaceutical ingredients, of which China is a major provider. The global sanctions against Russia resulting from its invasion of Ukraine disrupt imports that allowed Russia's biotech industry to thrive.

---

[118] "Putin met with Zhores Alferov," Kremlin Press Release, 18 April 2003. Available online at: https://www.kommersant.ru/doc/962103 (Accessed 29 July 2022)
[119] "Russia on Track to Remain World's Biggest Grain Exporter," The Moscow Times, 15 May 2019. Available online at: https://www.themoscowtimes.com/2019/05/15/russia-on-track-to-remain-worlds-biggest-grain-exporter-a65592 (Accessed 29 July 2022)
[120] Alina Osmakova, Michael Kirpichnikov, and Vladimir Popov, "Recent biotechnology developments and trends in the Russian Federation," New Biotechnology, 25 January 2018. Available online at: https://www.sciencedirect.com/science/article/pii/S1871678416326693 (Accessed 29 July 2022)

[121] Trade data collected from Comtrade (comtrade.com) and Datamyne (datamyne.com in late 2021 and early 2022.
[122] D. O. Kolevatykh, I. S. Selezneva, and M. N. Ivantsova, "Current State and Future Prospects of Biotechnology in the Russian Federation," AIP Conference Proceedings, 4 Febrauary 2022. Avaiable online at: https://aip.scitation.org/doi/abs/10.1063/5.0069055 (Accessed 29 July 2022)
[123] "Russia Pharmacuetical Market Trends in 2020," Deloitte CIS Research Center, 29 January 2021. Available online at: https://investinrussia.com/data/files/sectors/russian-rharmaceutical-market-trends-2020.pdf (Accessed 29 July 2022)

The global food market has already been impacted by the withdrawals of Russia's agricultural resources[124] and Russia is unable to maintain its medical supplies.[125]

Russia's chemical industry have long been suspected to be involved with the country's chemical weapon program. Several entities that were believed to support this program, have be placed on a U.S. Department of Commerce watchlist in early 2021.[126] A noteworthy aspect of this list is that it contains companies based in Germany and Switzerland, which extends the network into the global supply chain.[127] Companies trading dual-use chemical precursors and technology should practice due diligence to avoid being an unwitting accomplice to chemical weapons proliferation.

Take Aways

In both Russia and China, there is potential for the biotechnology and chemical sector to be misused to develop unconventional weapons. In the case of Russia, this concern chiefly focuses on the potential misuse of supplied equipment and chemicals, especially considering the existing infrastructure left behind by their covert bioweapons program. Dual-use chemicals being diverted from legitimate industry use to weapons programs is another concern that warrants attention. In the case of China, concerns are related to the potential for misuse of genomic information. Companies trading dual-use technology and resources should undertake enhanced due diligence, especially when dealing with either country. Companies holding genomic information should also implement bio cybersecurity best practices to safeguard digitized genomic information. Additionally, China's CDMO's attractive position to reduce the cost for research makes them a prime source for data generation. Researchers of dual-use concern topics should avoid using CDMOs for data collection so that the research cannot be leveraged for weapon development. Non dual-use topic researchers should also be vigilant with data agreements when working with CDMOs to limit opportunities for theft of research data.

---

[124] "Putin Ties Grain Exports to Demand That Sanctions on Russia Go," Bloomberg, 26 May 2022. Available online at: https://www.bloomberg.com/news/articles/2022-05-26/putin-ties-grain-exports-to-demand-that-sanctions-on-russia-go (Accessed 29 July 2022)

[125] "Fears in Russia Over Pharmaceutical Supplies," The Moscow Times, 9 March 2022. Avaiable online at: https://www.themoscowtimes.com/2022/03/09/fears-in-russia-over-pharmaceutical-supplies-a76840 (Accessed 29 July 2022)

[126] "U.S. Department of Commerce Adds 14 Parties to the Entity List for Support of Russian Weapons of Mass Destruction Programs and Chemical Weapons Activities," US Department of Commerce Press Release, 2 March 2021. Available online at: https://www.commerce.gov/news/press-releases/2021/03/us-department-commerce-adds-14-parties-entity-list-support-russian (Accessed 9 August 2022)

[127] "От «Новичка» возникло послевкусие. Санкции против малоизвестных компаний ударят больнее, чем кажется," Fontanka, 5 March 2021. Available online at: https://www.fontanka.ru/2021/03/05/69797849/ (Accessed 9 August 2022)

Telecommunications

The rapid exchange of information over vast distances has allowed for a global revolution in communications. This trend continues with the development of ever more sophisticated communications means such as quantum encryption, which has the possibility of protecting information from ever more powerful computers. Quantum cryptography uses the physics of the sub atomic world to safely transfer information with another person. In China, scientists have already built a sophisticated communications networks using fiber optic cables using the photons of a laser to send information.[128] These technologies have both economic and security applications and, as such, give material benefits to the states able to develop commercially viable products first.

In the China context, quantum communications technology is of special importance. In collaboration with foreign universities, and detailed further in case study 16, the PRC has developed a quantum communication network leveraging satellite technology and fiber optic cables for an encrypted network connecting Beijing and Shanghai.[129] This supposedly un-hackable encryption network with potential military applications did utilize several western microelectronics and parts but was developed under civilian pretexts. This example highlights the way MCF strategies are implicating the acquisition of foreign technology in the telecoms space. Outside of quantum communications and encryption, the PRC is incredibly active in commercial telecommunications applications with companies such as Huawei and ZTE. While both were the recipient of many American trade restrictions during the Trump administration, both actors are still active in the industry and in the supply of smartphone technology abroad. Additionally, Huawei and ZTE have been contracted for a number of BRI projects to supply internet infrastructure to foreign nations.[130] This poses any number of traditional diversion risks, but also creates concerns about the collection of data from citizens of foreign nations that could be utilized by the PRC.

In Russia, there is already budding interest in the potential applications of this technology to protecting sensitive information from outsiders.[131] The Russian Quantum Center at Skolkovo and Moscow State University's Center for Quantum Technology are domestic leaders in the field. Neither entity is sanctioned by Treasury, but the former

---

[128] https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/ and https://phys.org/news/2021-01-world-quantum-network.html

[129] https://www.nature.com/articles/s41586-020-2401-y

[130] https://e.huawei.com/en/solutions/industries/government/smart-city

[131] https://archive.ph/isItu#selection-141.0-146.0 and http://www.mathnet.ru/php/person.phtml?option_lang=rus&personid=121524 and http://www.mathnet.ru/rus/person48254

has listed export controls as limiting its ability to import critical components.[132] Russia has a strong cadre of physicists and mathematicians, particularly when it comes to basic science and theoretical developments. The leaders in this space for Russia are young, ambitious, and have the backing of the state and the country's elite research institutions.[133] However, corruption, and shortsighted political decisions by top leadership have meant Russia cannot domestically supply its scientists with the tools they need to develop the technology at scale.[134] Brain drain to the United States and Europe have weakened Russia's ability to compete at full strength in this specific space, according to stakeholders in-country.[135]

Takeaways

Russia is largely reliant on international providers or component manufacturers for its telephone systems, including its strategic and military systems. This is true for more traditional communications equipment, for advanced telecommunications equipment, and for novel telecommunications such as quantum communication. Given this, company's offering telecommunications equipment and components should closely scrutinize transactions to identify any Russian nexus and should refer cases to their national export licensing authorities.

China is more self-sufficient with regards to telecommunications equipment but is likely to continue to be reliant on components and semiconductors for communications equipment sought from the international marketplace. Some such components may be subject to export control and should automatically be referred to export license authorities. Where that is not the case, companies should undertake due diligence to ensure that the entities acquiring components and semiconductors are not linked to China's strategic or military programs and should avoid selling goods to untrusted distributors in China or to those entities abroad with linkages to said Chinese distributors.

Robotics

Robots are autonomous machines that carry out the often dull, dirty, and dangerous tasks traditionally assigned to human laborers. In the context of sectoral mapping, CNS examined robotics in the context of manufacturing, remote manipulation in areas where manual labor is dangerous for humans, and autonomous weapons systems. With both industrial and battlefield applications, these devices have direct applications to

[132] https://novayagazeta.ru/articles/2021/12/03/kvantovaia-gonka
[133] https://archive.ph/DncVj and https://www.youtube.com/watch?v=9dXwFuDl2_s&ab_channel=%D0%A0%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0 and https://www.nature.com/articles/nphoton.2017.57
[134] https://novayagazeta.ru/articles/2021/12/03/kvantovaia-gonka
[135] ibid

geostrategic competition as they convey economic and military advantages to the states able to wield them at scale.[136]

In the world of industrial robotics, advanced multi-axis machines are able to perform complex labor and manufacturing tasks. Such technologies if used at industrial scale and with precision could increase the manufacturing capacity of the relevant country. Russian entities such as Almaz Antey subsidiaries are working on multi-axis general use robotics arms. These robotic arms would provide Russia with the ability to replace humans with robots in production lines. Other applications for industrial robots include pick-and-place, a less sophisticated, but still important industrial task. For a country like Russia with a declining population and stagnating industrial base, the commercialization and wider application of industrial robotics could aid with managing its competitiveness.[137]

In the Russia context, the Russo-Ukrainian war has seen the extensive use of autonomous devices from both the commercial and military markets. These drones range in sophistication, and are often built and maintained using commercially available electronics, often from the United States and Europe. These drones have proven fruitful in both the creation of propaganda for the internet age and guiding munitions to target.[138] Russia has developed unmanned ground systems that have received a great deal of interest and boosting from Kremlin propagandists, however these technologies have found themselves of very little use in high-intensity combat and are relegated to the rear echelons.[139] Despite the massive manpower problems Russia faces in its attempt to conquer Ukraine, the use of robotics and drones remains relatively small.

Takeaway
Russian entities involved in its autonomous weapons projects may seek goods, software, training data (for machine learning) and know-how from abroad. Any approaches from Russian strategic entities should be referred to national export licensing agencies for advice.

Red Flags

This section draws together the due diligence elements identified from the analysis on this sectoral guidance.

Category	Red Flag	Source

[136] И. Л. Ермолов, Стратегические вопросы развития российской робототехники.
[137] https://www.youtube.com/watch?v=zhwODBHs6Zs&t=1s&ab_channel=FPIRussia
[138] https://asiatimes.com/2022/06/us-made-parts-keep-russias-artillery-firing-in-ukraine/
[139] https://www.newsweek.com/russia-uses-huge-demining-robots-clear-explosives-seized-city-mariupol-1709701

Company/Partner	Company is linked to the military or on a watch list Company operates in a strategic sector Company's website identifies problematic activity such as links to military end-uses and/or military end-users of concern Company is less than 5 years old Company has previous negative publicity for proliferation concerns Company is an authorized arms manufacturer or is listed as a strategic enterprise Company's website has a communist party page demonstrating its close links to the Chinese state.	Company website, LinkedIn, news media coverage, sanctioned entity lists (in particular, the China country section of the U.S> BIS Entity List, and the U.S. DoD's "Chinese Military Companies List" per Section 1260H of the NDAA of 2021; and the U.S. Treasury Dept. OFAC's "Non-SDN Chinese Military-Industrial Complex Company List (NS-CMIC List)).
Academic Involvement	Entity is a university in a country of concern (or identified explicitly on a sanctions/restricted party list or on the ASPI University tracker Entity has an academic program or laboratory in a strategic field and receives government sponsorship Entity has a known linkage to national laboratory researchers in a strategic field	University website; U.S. BIS Entity List; Japan Foreign End-User List, (maybe EU / UK) ASPI Tracker
Nature of Technology	Is the technology on a control list? Is the technology a chokepoint technology? Is the technology sought by a country of concern through a nationalized indigenization plan? Was a military-grade product sought for civilian purposes when a civilian-grade option is available?	Technology control lists, product order

	Does the technology feature in the sectoral analysis section of this guidance?	
Shipping	Destination in a country of concern, including great powers for strategic technology Vague delivery dates Odd destinations and/or unusual routing	
Illicit Involvement	Is there a lack of information on end use? Is the procurer an intermediary rather than an end user? Are they hesitant to provide information on the actual end user? Lack of company website or other official presence Cash payments for expensive orders that usually are financed Incomplete orders, shipments for specific parts	See also the distributors section below.
Geography and Third Country Diversion	Is a party to the transaction in a country of concern or contested territory like in Ukraine? Is the party based in Hong Kong (mostly relevant for China) or in a CIS country (mostly relevant for Russia? Is the destination in a location that is a hub for controlled activity? Does the end destination make sense for the product being purchased? Is the end destination a freight forwarding firm or other transshipment hub? Is the shipping route abnormal? Does the product make sense for the customer?	

	Is the packaging consistent for the product and destination? Can the country support the industry the technology is viable for?	
China Specific Red Flags	Company has a known link to the Thousand Talents Plan or similar recruitment agencies. Company is in a strategic industry and located in a domestic geographical hub near other entities in that industry. Is the end user one of the authorized military goods manufacturers or is it a strategic entity such as CASC, China Academy of Launch Vehicle Technology, or the Chinese Academy of Engineering Physics?	
Transaction	Routine maintenance or services declined by customer	

Compliance and Due Diligence

Due diligence efforts aim to take systematic and proportionate steps to identify compliance obligations and other risks related to a transaction or relationship. While companies must always be compliant with relevant laws, in reality, companies will make decisions on how to best match compliance resources available with the numerous, often competing, compliance tasks. Thus, this section addresses a variety of practices that capture the compliance process more broadly than what may be considered due diligence traditionally. While red flags do inform due diligence best practices, there are risk management strategies that are not expressly linked to red flag identification, such as entity screening. Through the implementation of strategies that identify new red flags and check against known ones, the two necessarily inform each other as nefarious actors develop new strategies that go undetected by current due diligence practices. Thus, due diligence strategies are always already being built upon and improved. It is worth noting that while this is aimed at compliance teams within the private sector, effective due diligence requires coordination between the government and industry to be most effective. For more information on what types of tools governments can provide, see the What States Should Do section in this guidance.

This section has three primary categories organized around different aspects of compliance – the company/partner, the technology being traded, and considerations for the transaction itself. Additionally, there is a section highlighting specific concerns surrounding academic and research institutes which are tech innovation hotbeds but get frequently overlooked. Each subsection contains a list of actionable due diligence best practices pertaining to the topic area as well as country specific considerations that inform the application of said practices. While some methods may be more cogent depending on the country in question, the methods listed can be applicable in a variety of compliance situations and should be considered for use more broadly. That said, the country specific considerations will provide insight into some current conditions that inform due diligence in an era of strategic competition. As always, a general awareness to security risks and industry developments, much of which is outlined throughout the rest of this guidance, will be essential to employing these due diligence strategies successfully.

Company / Partner

The goal of company / partner due diligence is to identify legal, reputational, and associated risks of cooperation with the entity. This includes ensuring you are looking at the correct entity, understanding its structure, ownership and control status, identifying any past activity of potential concern (including relationships with entities or programs of concern), and identifying any red flags.

Category	Element	Source
Nature of the company	Is it a distributor? Is it sanctioned? Is it involved in strategic technologies such as nuclear, arms or missile development? Is it an authorized procurement agent for programs of concern?	A due diligence survey completed by the company or partner could surface some of these points. The other points in this table can also help to get at these points.
Company Website	Do they have a website? Not having a website is a potential red flag. Does the native language version of the website include a 'party' page or otherwise detail connections with programs of concern?	Company's website identified through web search or by company itself. Many websites have a native language tab. When accessed via google chrome, google translate can be used to read this native language site in your own language.

	Does an image search for the company's domain reveal images of activities of concern?	In Google, searching for site:www.xxxx.xx then hitting the 'images' tab will show all images on the company's domain
Past activity	Does the company have a history of work implementing contracts for government entities? Does the website mention problematic activity to include government contracts; does the website have photos of military, equipment or imagery that indicates involvement in military-related projects; does the website mention links to government initiatives such as 5-year plans; is the website simply not accessible outside the country of concern? Is there other information about past activity of concern (see the news and media section below too)	Official data sources concerning governmental contracts. Many corporate due diligence services and websites can be used are tooled for different regions of the world. Please reach out to CNS for recommendations. Company's website in English and original language (noting that original language websites often contain more information). Company's website may mention past projects or awards.
Ownership and Control	Is the entity privately owned or controlled by a foreign government's state-owned enterprise? Is the company owned or controlled by a sanctioned entity? Is the company a subsidiary of a state-owned entity?	• Company registration documents, • relevant company registers (provincial registries in China, national registry in Russia), • Third party services.
Social Media	Does the company have a presence on LinkedIn or equivalent regional social media sites?	For determining if a company exists, the existence of a credible profile is usually sufficient.

	Does the company's social media show involvement in strategic projects?	Company logos are usually used on social media and will often depict a strategic item (missiles, nuclear etc.) if the company is involved in that sector. Conducting media searches (i.e., for photos) linked to the company's account is a good way to identify past projects.
News and Media	Are there news stories of the entity in question being involved in illicit transfers Are there news stories of the entity developing weapons for the military? Is there news of the entity winning government contracts and awards?	Use of advanced search engine techniques to search domains such as .cn or .ru using the name in Chinese or Russia characters. Use Google but also relevant national search engines (Yandex and Baidu) For more information on this, see Annex 3. Searching for the company name plus words like 'defense' or 'military' can also identify connections of concern.
Location of the company	Is the entity or claimed end-user located in a non-European former Soviet republic or Hong Kong? Some former Soviet republics, particularly in the Caucuses and Central Asia are increasingly being used as transshipment points to Russia, including the Russian government. Is the entity co-located with an entity of concern?	Use best judgement in determining who the end user is or could be. Age of the company, purpose, declared end use and other factors must be used in combination with geography. Geography is a risk factor, but not a determiner. Identification of co-locations of concern can be challenging. However, it is worth Googling the address to see if webpages mentioning the address come up and looking at the address in Google maps (or national equivalents such as Baidu) or Yandex maps. Each of these mapping services can show the names of businesses overlayed on the map.

China Specific Considerations

Entities within the PRC use several strategies to obfuscate the identity of the end user or end use. This is largely due to the MCF nature of their economy when it comes to strategic goods. When performing due diligence for transactions relating to China, mentions of 'convergent technology' or 'special projects' are strong indicators that the entity is involved in MCF activities, and the transaction could end up with a military end use. This is also a useful method to assess if the company has empirically been a recipient of government or military awards. One of the most effective means to mitigate against these forms of transactions will be to cross-reference the English version with the Chinese version of the websites. Many times, companies will try to obfuscate their links to military or government contracts on the English version of the website when attracting business but in turn herald their connections to the government for a domestic audience. Additionally, checking for official military procurement tender announcements in the PRC can help identify the recipients of both present and past contracts.

To this end, one of the most effective measures a company can take towards its compliance efficacy is to have a member of the compliance team fluent in Mandarin or with enough working knowledge of the language to detect these discrepancies. It is also common for there to be many Chinese companies with similar names that can be confused for the entity engaging in the transaction. This is just one area where Chinese language skills on a compliance team could be essential in conducting effective due diligence. This said, it should also be noted that a lot can be achieved simply using Google translate. Additionally, Wikipedia is often a good source of an entity's name in Chinese characters (which can be verified by inserting the name into google translate). Conducting searches using these Chinese names is often revealing.

Some additional considerations when researching an entity that can help inform whether to pursue business with a Chinese entity include checking for references to the Thousand Talents Plan which has been used to recruit researchers in strategic fields. Lastly, because the PRC leverages its university system as part of general MCF strategic technology development, it is valuable to see if companies have connections to academic institutions which may, in turn, have connections to the government or military. Alternatively, it is useful to determine if the company is founded by former professors as much of the start-up space in China is tied to MCF and are commonly outputs from former university projects.

Russia Specific Consideration

Russian entities do relatively little to hide their links to military and dual use entities. The links to these institutions are often advertised on the home page of their website or can be identified through other corporate data widely available in Russia. Since Russia's February 24th invasion of Ukraine, some Russian companies have blocked their websites to users outside of the Russian Federation. This is often a good indicator that a company is doing business with, or is itself, a sanctioned entity. When Russian entities do attempt to obfuscate their links to military or dual use institutions, they are often third

party wholesalers of goods. An advanced web search of the entities name in Russian alongside relevant search parameters can be used to identify these links or auditing services as much of this information is public and available on the open web. This web search must be done in the Russian language or it will not pull the relevant results.

Due to the customs union with Kazakhstan and Kyrgyzstan, procurement of dual use goods is reportedly increasingly happening through these channels. This creates complications as the data available is still small. Critical judgement and know-your-customer procedures such as why a newly formed corporation in Kyrgyzstan is ordering large amounts of electronics or milling machines can help companies avoid legal and reputational risks. More sophisticated operations mask their ownership in weakly regulated U.S. jurisdictions such as Delaware. In this same vein, services are increasingly being created that openly and actively advertise their intent to buy goods to evade sanctions. At least one site reviewed by CNS had a map on their website showing the countries they use to transport goods into Russia and around sanctions. Company ownership, age of the company, requests for goods in bulk and other basic due diligence procedures when reviewing business in Russian allied or partnered countries is just as relevant as if doing business with a company inside the Russian Federation.

Nature of Technology

Category	Element	Source
General technology	• Assess if the technology in question is dual-use or strategic in nature, even if it is not explicitly on a control list. This could include determining whether it is relevant to the types of strategic technology that Russia and China are seeking to indigenize.	Technical datasheets, scientists and engineers with knowledge of the product
Control lists	• Identify of the technology being traded is controlled on a current control list. • Identify both physical and digital components of the technology that may be subject to control.	Technical datasheets, scientists and engineers with knowledge of the product
Cybersecurity	• If there is a digital component of the technology, implement appropriate cyber-security standards both	Potentially useful standards: NIST 800

	internally and when transferring the technology.	
Nature of technology	• Determine if the technology being purchased is used in the manufacturing of other strategic goods.	

China Specific Considerations

For the PRC, strategic technology development is more than just a commercial endeavor but also part of the national strategy, outlined by various Five-Year Plans (FYP). As the name suggests, these policy doctrines are released every 5 years and outline the goals for the government. This has included for the last 10 years or more an intentional effort towards indigenization of strategic technologies. These are outlined further in the specific FYP on science and technology. These categories are captured in detail throughout the earlier sections of this guidance. For the purposes of this section, it is simply worth noting that the technology areas the PRC is most intent on developing for strategic purposes are by and large publicly noted. Especially for professionals working in compliance in one of these strategic industries, considerations on the nature of the technology within the broader scope of Chinese indigenization efforts is essential to effective due diligence.

Because the end-goal of the Chinese national strategy is to be self-reliant, it is especially critical that technologies which are used to manufacture additional advanced strategic goods are subject to control. This report outlines specific 'chokepoint technologies' which are technologies which the PRC does not currently have indigenous capability for, but should they obtain said technology, would be able to produce advancements in areas beyond the specific technology itself. The best example of this, detailed further in the Computing section above, is the interconnect technology required to scale up the processing power of supercomputers.

Not all these technologies will be on control lists as the sectors naturally progress faster than the lists do in many cases. Thus, it will be important for entities to use their technical expertise within the sector they operate to help define what these technologies are over time and limit the export of such strategic goods. Inter-industry coordination in this regard will be useful for creating future standards for due diligence.

Lastly, many modern strategic goods have both digital and physical components. While historical export control best practices focus on the security of physical goods, companies must implement effective cyber security standards on digital elements of transactions, so they are not diverted towards nefarious end uses. Common areas where this is most impactful are machine learning and additive manufacturing where digital

files and algorithms are just as essential to the operation of the technology as the physical component being exported.

Russia Specific Considerations

Russia has spent a great deal of time, effort and money to rebuild itself as a technological powerhouse. Much like the Chinese government, the Russian government has put forward several strategies to make Russia 'great again'. The core of this is development of a business-friendly space people want to live and create new innovations in. However, while Russia produces excellent programmers, mathematicians, physicists and scientists, it has trouble building things. As such, most of the technology supporting Russia's cutting-edge technology advancements are reliant on Western goods and services. Russia is currently struggling to achieve its proposed aims as hundreds of thousands of highly skilled workers flee a situation inside Russia which they view as increasingly unsafe or untenable. Since February 24th, many Russian companies have relocated offices to Armenia either to protect the safety of their employees, avoid sanctions, or both.

As such, the question of what constitutes a Russian company can be a grey area for due diligence officers. Goods relevant to various emerging technologies, such as those powering research on quantum computing or machine learning need to be critically analyzed. Two questions which are vital to ask are: why does this company need this product? And, is there risk of diversion of the good into the Russian Federation? There is no legal or moral reason to suspend all ties with Russian nationals or Russian nationals doing interesting research and development. But basic knowledge about potential business partners is vital to making informed decisions.

On the less sophisticated scale, the Russian military has become very adept at importing goods that while technically are not on control lists or considered dual use, can be adapted to those purposes. Businesses must be aware of links between their partners and Russian military contractors who build weapons and communications devices. Even if a good is not controlled, one can incur severe reputational damage if even outdated technology is diverted for non-civilian purposes.

Transaction

This section identifies due diligence steps that should be taken in relation to each transaction. This section focuses on measures that should be taken over and above the company / partner due diligence as detailed above.

Category	Element
Shipping	• Confirm that shipping practices are standard for the type of product and

	region. This includes shipping routes, end destinations, etc.
Shipping	• Check that the shipping destination is not another transshipment hub.
Shipping	• Confirm that the dimensions of the package (weight and size) are appropriate for the order when finalizing shipping preparations of sensitive technologies.
Geography	• Is the purchasing entity in a country of concern?
Third country diversion risks	• Is it first being shipped to a known diversion hub?
Finance	• Avoid cash payments for orders that are usually financed with other instruments.
Finance	• Confirm that the paying entity is the same as the one placing the order and receiving the shipment?
Finance	• Confirm that the financing is not through a state or military grant.

China Specific Considerations

When assessing the transactional factors in a Chinese context, there are a couple of important considerations.

First, when considering shipping and geography, there is primarily a need to be cautious of transactions that go through territories such as Hong Kong and Macau as these locations may not be the ultimate destination but frequently have less serious barriers to trade than with the mainland. Because of the number of Chinese entities with subsidiaries in these territories, one aspect of due diligence should be understanding the risk of a subsidiary company ordering an item into Hong Kong and then sending it to the main office in mainland China.

Last, there are not too many unique concerns when it comes to financing. The main goal of due diligence in this regard is to confirm that the government or military is not the

financing agent for the organization or the specific project. There are domestic databases in the PRC where these government contracts and tenders are sought and distributed. However, accessing these databases can be difficult when outside of the country due to the firewall and require mandarin language skills to navigate. Alternatively, many company websites will highlight the fact that they won this award. When checking the entity websites, it is important to note any mentions of grant or project-based work for the government or military as these are signs the organization engages in MCF behavior.

Russia Specific Considerations

Given Russia's current financial isolation, almost all financial transactions to Russia currently involve some sort of suspicious behavior such as the use of cryptocurrency or multiple banks. Likewise, the use of fronts, bank accounts in third countries and other behaviors traditionally associated with money laundering are increasingly required to acquire even non-export controlled goods for Russian companies engaging in legitimate transactions.[140] As such, it is extraordinarily difficult to identify suspicious transactions, and beneficial ownership when all transactions are suspicious. Likewise, Russians will use "sanctions" to refer to export controls, financial blocking and self-imposed restrictions by companies. The resulting confusion makes it difficult, if not impossible, to discern craftiness from illegality even for the people involved in the transactions themselves.[141]

This is compounded by the unknown number of Russian companies opening fronts in countries like Turkey and in Central Asia and other locales for the purposes of getting around banking restrictions that are legal under the U.S. sanctions regime. The scope means that again, behaviors traditionally associated with evasion and money laundering are used for the purchase of non-controlled, non dual-use goods. The use of a front in Turkey or a former Soviet Republic to transact may be functionally required for doing legitimate business with Russian companies, but opens the participants up to enormous and unknown risks given the fluidity and opacity of the overall situation. There are acute financial risks as well that money could be stolen or not reach its intended destination given the number of new financial instruments to avoid sanctions that have emerged. Social media postings by the few remaining foreign expatriates in Russia indicate a wild-west atmosphere where money can go easily missing.[142]

A core part of doing effective due diligence in the Russian context is a proper team with professional fluency in the Russian language. Many of the connections between certain entities and the military or security services are obvious to those with the language

[140] See Usmall.ru and the litany of other new businesses designed to get around "sanctions" https://usmall.ru/
[141] Interviews with Russian nationals attempting to flee Russia 4/2022
[142] Social media postings in closed Moscow expatriate help board.

skills and regional experience, but difficult, if not impossible to decipher without proper experience with Russian business culture and bureaucracy. Given the ongoing war and continued high-profile attacks on civilian targets by the Russian military, businesses entail extreme reputational and legal risks for doing business with Russian entities and getting it wrong.

Dealing With Academic and Research Institutes

The focus on emerging technologies in the context of great power competition brings into focus the role of universities and research institutes. While the popular image of a university is a place in which students are taught and theoretical research conducted, the reality in most countries is that universities and research institutes are closely tied into the country's commercial sector and national technology science and technology plans. This is true as much in Russia and China as it is elsewhere. Given this, engagement with academic and research institutes is a key pathway through which technology transfer and proliferation can occur. There is a need for due diligence when dealing with Chinese and Russia universities and research institutes. Case studies 4 and 16 showcase two different ways the PRC has leveraged university collaboration. In the first case, a professor is recruited to do research abroad for the PRC at a foreign university. In the second case, university collaboration resulted in the transfer of dual-use goods to the PRC under the auspices of academic collaboration.

Category	Element	Source
Departmental or staff connections to government labs or dual-use start-ups.	• Identify any connections the entity may have to academic institutions (or their operators) in a country of concern. This can include staffed professors/researchers, joint research, start-ups with a connection to academic programs, etc.	Use the university's website to see if staff or professors in a department have a dual-hat with military or security-linked entities. Critically approach who funds research at which faculties and departments in the institution. Academic institutions are sprawling and often isolated from one another. A handful of professors in one science faculty being tied to a government entity or lab does not mean another faculty in the humanities cannot

		be engaged with for the purposes of humanitarian work or citizen diplomacy.
Finance	• Confirm that the financing of the research, grant, or exchange, is not through a state or military grant.	Due diligence information - ask the foreign partner.
Intellectual property and the right to publish	Restrictions on publication and data. If contractual conditions prevent publication, it is likely not basic scientific research as the client is paying for proprietary information.	Review the contract

One helpful resource for identifying universities of possible concern is the ASPI university tracker. However, effective use of academic repository metadata sites such as Scopus, the Chinese site CNKI, and the Russian site e-library can also be used to identify universities undertaking military-related research.

Potential Additions to ICPs

ICP guidance generally identifies 7 elements as detailed below. This section seeks to identify specific additions to ICPs.

Common elements of an ICP[143]

- Top-level management commitment to compliance
- Organization structure, responsibilities, and resources
- Training and awareness raising
- Transaction screening process and procedures
- Performance review, audits, reporting and corrective actions
- Recordkeeping and documentation
- Physical and information security

Many of the following elements would be associated with a number of elements in the generic ICP structure detailed above and relate to thematic pillars of ICPs such as customer onboarding, transaction screening, business travel, and cybersecurity.

Customer Onboarding

[143] See for example https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN

- Ensure due diligence and disclosure measures require all available information necessary to establish that a counterparty is not involved in the military end use enterprise. This may include names of board of directors, lists of subsidiaries and parent companies, names of major investors, and other data.

Hiring

- Ensure the hiring process includes contractual information including strong non-disclosure agreements and policies restricting removal or unauthorized transfer of company property or sensitive data.
- When conducting background checks on potential hires, seek to identify links with Chinese military linked entities and Russian strategic entities. Refer concerns to relevant export licensing authorities.

Travel

- To address the potential vulnerability that business-related foreign travel can present, when possible, sanitize all electronics to remove intellectual property or personal information before traveling overseas, and check electronics after return.
- Require staff to liaise with compliance officials before giving external presentations on technical topic related to controlled or emerging technology.

Physical Security

- Monitor visitors if they are given access to areas containing sensitive technology, products, or personal information.

Audit

- Establish internal audit processes to ensure ongoing compliance verification and early detection of unauthorized technology transfers or IP theft.

Whistleblowing and Reporting

- Ensure whistleblower protection policies are in place and available to report issues related to theft of intellectual property or diversion of technology.
- Ensure appropriate and effective consequences for violation of disclosure requirements and engagement that do not align with company policies.

Cybersecurity

- Ensure physical security personnel and information technology security personnel have sufficient expertise, threat detection software, countermeasure tools, and protective processes in place.

- Establish and maintain effective data security measures to improve data security, internal breach prevention, incident response processes, and maintain compliance with relevant requirements.

Use of Distributors

Distributors are widely used by manufacturers to reach markets that they would not otherwise be able to penetrate. Russia's and China's need to acquire a wide range of controlled and noncontrolled technology for their strategic programs highlights the particular risk that distributors could be used by those countries as routes through which to acquire western technology that would not be sold if the approach was made directly to the manufacturer. In this document, repeated use is made of the term 'trusted distributor', implying that distributors should not be used unless trusted. Trusted in this context is an imperfect term but is meant to convey that the manufacture has confidence that the distributor will conduct an equivalent level of due diligence as the manufacturer would and would reach a comparable decision on whether or not to undertake a transaction. In practice, companies must be wary of the use of distributors. For many controlled goods, there is an expressed expectation that the goods not be sold through distributors. Even when use of distributors is permitted, there are documented cases in which distributors have been complicit in shipping goods to prohibited end uses for additional profit. [144]

Particularly in relation to Russia, companies should exercise caution in relation to distributors that are Russian owned or controlled – regardless of where in the world they are – and where a distributor is located in Russia's near abroad and specializes in selling into the CIS market. In both cases, there are recent examples of distributors shipping western-origin goods to Russia's strategic programs without the knowledge of the manufacturer.

Good practices for use of distributors including some level of transparency around to whom the distributor is shipping (recognizing that the distributor may wish to keep this confidential so as to ensure the manufacturer cannot bypass them in selling to clients), some level of training and audit on the export compliance by the distributor, and a formalized commitment from the distributor about the sanctions and export control approach they are to take.

[144] See for example, "Chinese Citizen's Involvement in the Supply of MKS Pressure Transducers to Iran: Preventing a Reoccurrence", Available online at: https://isis-online.org/uploads/isis-reports/documents/MKS_China_30Apr2014-final.pdf (Accessed 1 August 2022)

Conclusion

Both the People's Republic of China (PRC) and the Russian Federation use a variety of similar means to obtain foreign technology and expertise. These means run the gamut from sophisticated schemes using front companies, to means as simple as directly procuring a good or technology from the commercial market. The PRC, however, also heavily utilizes university settings and recruitment tactics aimed at attracting expertise to the country in ways in which the Russian Federation is not as active.

Emerging technologies from the commercial world are increasingly setting the pace of military development. Dual use emerging technologies such as drones, advanced semiconductors, and so-called hypersonic flight technologies increasingly find themselves used in militaries. The development of technology is undergirded by international cooperation and inter-connectedness between nations. This trend will continue in the turbulent era in which we now find ourselves. It is vital that industry and government continue to collaborate on licensing and vetting the transfer of technology and expertise to the PRC and Russian Federation. It is likewise vital that companies continue to invest in robust due diligence practices and keep up to date with new trends so that they can recognize and act upon red flags.

Annex 1: Case Studies

Case Study 1 – Insider Steals Advanced Microchip Technology[145]

The semiconductor market is quite competitive and any advancement in technology could set you ahead of peers. This incentive drove employees from United Microelectronics Corporation, Inc. (UMC), a Taiwanese foundry company, to steal trade secrets from the American company Micron Technology, Inc. (Micron). In 2018, the FBI linked the representatives at UMC to the PRC's state-owned semiconductor firm Fujian Jinhua. The technology in question is the Dynamic Random Access Memory (DRAM) used for advanced chip production that was developed by Micron. This DRAM technology was previously something both UMC and Fujian Jinhua did not possess.

Prior to the acquisition of trade secrets from Micron, Chen Zhengkun, a.k.a. Stephen Chen, a senior VP of UMC, negotiated an agreement with Fujian Jinhua to develop DRAM technology for Fujian Jinhua. Chen hired developers He Jianting, a.k.a. J.T. Ho, and Wang Yungming, a.k.a. Kenny Wang to aid in the development of this DRAM technology. Ho and Wang brought with them confidential information from Micron's Taiwan-based subsidiary. This was flagged by UMC's IT department because of the IP found on Ho's computer. Afterwards, Chen issued the researchers 'off network' laptops to continue doing research with the American IP from Micron. This resulted in specific changes to the design of UMC's DRAM chips, as was recorded in a file on Wang's laptop.

The resulting investigation by Taiwanese officials found only one of the off-network laptops in question. The other, as well as hard drives, papers, notes, and a phone, were disposed of by an unnamed UMC coworker of Wang and Ho's. In the early stages of the investigation, Chen Zhengkun fled to mainland China where he is now the president of Fujian Jinhua and in charge of its memory production facility.

Case Study 2 - Former Classmates Coordinate Economic Espionage[146]

Chinese national, Hao Zhang, was convicted in the United States of economic espionage and theft of trade secrets for his operations involving American companies Avago and Skyworks. From 2010 to 2015 he coordinated with co-conspirators from Tianjin University in China to take the IP from Avago and Skyworks and recreate the optoelectronics equipment for his own company domestically in China. According to the justice department report, Zhang was focused on stealing Surface Acoustic Wave

---

145 https://www.justice.gov/opa/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned

146 https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy

(SAW) and Bulk Acoustic Wave (BAW) filters which are used in wireless devices to eliminate interference from other devices and signals.

The particular technology in question relates to the Film Bulk Acoustic Resonators (FBAR) developed by Avago that allows for smaller and more efficient devices. These FBAR filters are dual use and are used in military and civilian communications technology. Zhang had an accomplice, Wei Pang, who worked at Avago at the same time as him. Both were involved in the coordination with Chinese Tianjin University and in 2009, they had relocated to China. This relocation plan was facilitated by officials from Tianjin University and was slated to result in the formation of another company, Novana, in the Cayman Islands. Novana was to be a competitor company to Avago and Skyworks for FBAR technology.

Case Study 3 - Provincial Ministry of Security Involved in Hacking Scheme[147]

The PRC has many instances of economic espionage but very rarely are they linked directly to government organizations as explicitly as in 2018. In this instance, hackers and insiders were alleged to be working for the Jiangsu Province Ministry of State Security (JSSD). This branch of the Chinese Ministry of State Security represents the Jiangsu Province, the capital of which is Nanjing. The PRC tends to have hubs for specific industries in specific provinces as part of their military-civil fusion strategy. Jiangsu Province is known for exporting electronic equipment and other high-tech goods and it one of the wealthiest provinces in China.

The Department of Justice states that the JSSD hired a team of hackers comprised of Zhang Zhang-Gui, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei, and Ma Zhiqi. Their primary responsibility was to steal technology related to turbofan engines, namely those used in commercial aircraft. To facilitate this, the group hacked into a French aerospace manufacturer's office in Suzhou, Jiangsu Province. Additionally, this engine technology was in development with American aerospace manufacturers which meant the hackers were able to gain access to other companies involved in the manufacturing of the turbofan engine.

These hacks included companies in three states: Arizona, Massachusetts, and Oregon. During the investigation, justice department officials concluded that a separate Chinese state-owned enterprise working in aerospace was working to develop a similar engine. According to the justice department, the hackers used the following methods to intrude companies and steal their data: "spear phishing, sowing multiple different strains of malware into company computer systems, using the victim companies' own websites

[147] https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

as ‘watering holes’ to compromise website visitors’ computers, and domain hijacking through the compromise of domain registrars.”

While the team of hackers was the primary tool used to obtain this information, the operation included efforts to recruit members of the U.S. Army to cooperate with JSSD intelligence agents as well as employees of foreign companies. In the instance of the French company based in Suzhou, two employees named Tian Xi and Gu Gen were recruited by the JSSD to employ malware onto the network in the Suzhou office. When the malware was discovered, “conspirators Chai Meng and Liu Chunliang tried to minimize JSSD’s exposure by causing the deletion of the domain linking the malware to an account controlled by members of the conspiracy.”

Lastly, Zhang Zhang-Gui was charged, as well as his co-conspirator, Li Xiao, with supplying malware used to hack Capstone Turbine. Li used the malware, amongst other things, to repeatedly intrude the networks of Capstone and a San Diego-based IT firm.

Case Study 4 - Professor and Former NASA Researcher Linked to Thousand Talents Plan[148]

A professor at Texas A&M University, Zhengdong Cheng, was indicted for failing to disclose his links to the Chinese Thousand Talents Progarm. He was leading a team of students to perform research for NASA. This government funded grant research had a stipulation that prohibited any collaboration with Chinese universities or Chinese owned companies. Cheng, however, failed to disclose his prior association with Guangdong University of Technology in China and his association with the PRC’s Thousand Talents Plan.

The Thousand Talents Plan is a structured recruitment organization in the PRC used to systematically attract and conscript human capital from foreign countries to attend school in the PRC and/or to work in the PRC following graduation. The implication is that students receiving an education in China would contribute to the workforce in a strategic technology field and close the gap between economic ambitions and the size of the workforce educated enough to grow strategic industries.

Dr. Cheng supposedly used his access to NASA resources at Texas A&M to leverage a higher position at Guangdong University of Technology.

[148] https://www.justice.gov/opa/pr/nasa-researcher-arrested-false-statements-and-wire-fraud-relation-china-s-talents-program

Case Study 5 - Health Researcher and Ohio State Professor Connected to Thousand Talents Plan[149]

Song Guo Zheng, a professor of rheumatology at The Ohio State University, was indicted for using around 1.4 million in grant funding from the National Institute of Health to perform research he intended to take with him to China. He was interdicted and arrested on a flight May 22, 2020 in Alaska while it was on a layover before it was intended to travel to China. In addition to the misuse of government funds, he was charged with making false statements about being employed by Chinese universities at the same time he was researching at American universities.

The investigation alleged revealed that Song Guo Zheng had been connected to the Thousand Talent Plan and that he only prepared to flee the country after he became aware of an internal investigation begun by his employer. According to the report, Zheng had been funneling his research into the PRC since 2013.

Case Study 6 - Clinic Researcher Linked to Thousand Talents[150]

Dr. Qing Wang, a researcher at the Cleveland Clinic Foundation, allegedly used more than 3.6 million dollars in grant funding from the National Institute of Health to conduct research. The case alleges that while employed at the Cleveland Clinic Foundation, he was also the Dean of the College of Life Sciences and Technology at the Huazhong University of Science and Technology in China. While employed at both of these institutions, he had received grant funds from the National Natural Science Foundation of China to perform similar research to the work he was conducting for the Cleveland Clinic Foundation.

In addition to this, Dr. Wang was affiliated with the Chinese Thousand Talents Plan. According to the justice department report, after Dr. Wang agreed to join the Thousand Talents Plan, the facilities of the college he was the dean of in China got $3 million in support from the Chinese government to upgrade research facilities. Dr. Wang also received free travel on his trips to China as well as an apartment on campus provided by the PRC government.

A year after these charges were raised, the USG dismissed these charges. It is uncertain why the charges were dismissed; however, this case still exemplifies how university collaboration, and the Thousand Talents Plan, are intricately linked to the PRC's efforts to further strategic research and recruitment.

---

149 https://www.justice.gov/opa/pr/researcher-charged-illegally-using-us-grant-funds-develop-scientific-expertise-china

150 https://www.justice.gov/opa/pr/former-cleveland-clinic-employee-and-chinese-thousand-talents-participant-arrested-wire-fraud

Case Study 7 - Former Employee Falsified Reports to Transship Goods to Iran and China[151]

Cheng Bo, a.k.a. Joe Cheng, a US-based former employee of Avnet Asia Pte. Ltd., a Singapore-based company specializing in electronic components and software, allegedly falsified documents in order to ship export-controlled power amplifiers to the PRC, and previously Iran. He was indicted in the US as a result.

Cheng was a sales account manager who represented Avnet's interest with a Hong Kong-based customer which Cheng was affiliated with. Cheng then fabricated documents in order to export power amplifiers of US origin to Hong Kong, knowing they would be transshipped from Hong Kong to the PRC. The Department of Justice alleged that from 2012-2015 Cheng was involved in 18 separate shipments that were transshipped in the same way. The shipments totaled almost one million dollars' worth of equipment.

A separate, unnamed sales manager for Avnet, based in Singapore, operated similarly and alegedly shipped goods to Iran and China over 29 unique shipments valuing at least $347,000.

While the criminal investigation is still under way, Avnet Asia has admitted liability for its employee's conduct and has agreed to pay over 3 million dollars in settlement.

Case Study 8 - State Security Ministry Hacks 12 Target Countries[152]

From 2011 to 2018, the US Department of Justice allege that the Hainan State Security Department (HSSD) recruited hackers and linguists in China to create malware used to hack into companies from 12 different countries and across multiple industries. Those identified from the HSSD that led the group are Ding Xiaoyang, Cheng Qingmin, and Zhu Yunmin. The targeted trade secrets included genetic sequencing technology and data, chemical formulas, technologies used in submersibles and autonomous vehicles, and information used to secure contracts in third party countries. The countries implicated in the case include the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland, and the United Kingdom.

To achieve these goals, HSSD established a front company named Hainan Xiandun Technology Development Co., Ltd., which operated out of Haikou. This front company was managed by a Hainan-based university. Other universities were also involved through recruitment of hackers and linguists identified by HSSD. This particular group

---

[151] https://www.justice.gov/opa/pr/chinese-national-charged-criminal-conspiracy-export-us-power-amplifiers-china

[152] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

of hackers has since become notorious due to their involvement in a number of different cases.

Justice Department reports[153] indicate that in order to begin a hacking operation, the organization would use spearphishing emails with mimicked legitimate domain names.[154] This was occasionally followed up by additional internal phishing campaigns, leveraging the access they had gained from the first round of phishing emails.

Lastly, the hacking group would use 'anonymizer services' to access malware inside the target company's networks. Namely, they used a Dropbox specific API command to steal data directly from in-network Dropbox accounts and obfuscate the download by making it appear legitimate.

Case Study 9 –Chinese Circuit Company uses Front in the US in Attempt to Illegally Export MMICs to AVIC in PRC155

The Department of Justice states that Shih, a California resident and former president of Chengdu GaStone Technology Company (CGTC), was indicted for attempting to steal monolithic microwave integrated circuits (MMIC) from a US based company to ship back to China for reproduction by CGTC. Shih used a front company he operated called Pullman Lane Productions, LLC. Pullman was being financed by the PRC government for the acquisition of MMIC technology.

Shih used an associate to pose as a US-based consumer of MMIC chips to gain access to the network of the target company. He planned to use the US-based company to transship the MMIC chips to the PRC, specifically the state-owned enterprise AVIC. The MMIC chips in question have dual use applications in missile guidance, radar, and electronic warfare. Kiet Mai, the associate involved in this front was also convicted of smuggling. Shih had Mai pose as a domestic consumer so they could gain access to the company's web portal and take proprietary information and pass it onto AVIC.

Shih has since been convicted of conspiracy to violate the International Emergency Economic Powers Act and the Export Administration Regulations. He was sentenced to over five years in prison and fined $660, 000 for his plans to export the sensitive technology. Chengdu GaStone Technology Co. was also placed on the Entity List of the US Department of Commerce for illicit procurement.[156]

---

[153] Ibid.
[154] Ibid.
[155] https://www.justice.gov/opa/pr/electrical-engineer-sentenced-more-five-years-prison-conspiring-illegally-export-china
[156] https://www.electronicdesign.com/technologies/analog/article/21171807/microwaves-rf-usmade-mmics-not-immune-to-illegal-export

Case Study 10 - Raytheon Employee Illegally Exported Missile Guidance Technology and Data to China[157]

Wei Sun had been an employee of Raytheon Missile and Defense for 10 years before attempting to illegally transport proprietary technical information out of the country and into China. In 2018, ahead of international travel Sun had requested to take a company laptop on his travels. Raytheon denied the request. Raytheon officials say the request was denied because Sun was working on an ITAR controlled project.[158] Despite being instructed not to bring his company laptop, the next month in January of 2019, Sun accessed his laptop from outside of the US and emailed a letter of resignation.

Sun eventually returned to the US where he was questioned. The investigation found that Sun had visited China, Cambodia, and Hong Kong, though he had initially reported he had been to Singapore and the Philippines. Ultimately, he was sentenced to 38 months in prison for delivering sensitive missile technology to China in violation of the AECA and ITAR for being exported without a license.[159]

Case Study 11 – 'Technology Spy' Recruits US Citizen for Engine Technology Theft[160]

In 2016, Wenxia Man, a.k.a. Wency Man, was convicted of conspiring to export defense articles, namely jet engines used in the F-35, F-22, and F-16, without a license.[161] The attempt was thwarted before the technology could be delivered to her contact in the PRC, Xinsheng Zhang, who Man described as a "technology spy" [162]aiming to replicate technology stolen from other countries. Man said the man was especially interested in stealth technology.

Man attempted to export the following engine models: "Pratt & Whitney F135-PW-100 engines used in the F-35 Joint Strike Fighter; Pratt & Whitney F119-PW-100 turbofan engines used in the F-22 Raptor fighter jet; General Electric F110-GE-132 engines designed for the F-16 fighter jet; the General Atomics MQ-9 Reaper/Predator B Unmanned Aerial Vehicle, capable of firing Hellfire Missiles; and technical data for each of these defense articles."

---

[157] https://www.justice.gov/opa/pr/former-raytheon-engineer-sentenced-exporting-sensitive-military-related-technology-china

[158] https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-sun.pdf

[159] Ibid.

[160] https://www.justice.gov/opa/pr/california-woman-sentenced-50-months-prison-conspiring-illegally-export-fighter-jet-engines

[161] https://www.reuters.com/article/usa-china-exports/u-s-woman-convicted-of-conspiracy-to-export-jet-engines-to-china-idUSL1N1912M0

[162] Ibid.

Case Study 12 – Hong Kong Front Company Linked to Export Conspiracy for PLA Navy[163]

Ge Songtao was the chairman of Shanghai Breeze Technology Co. Ltd., a Shanghai-based company that specializes in marine equipment. For the advancement of his own company, Ge was looking to source "combat rubber raiding craft equipped with engines that could operate using gasoline, diesel fuel or jet fuel". Ge leveraged an employee based in the United States named Yang Yang. Yang was instructed to order the gasoline engines that were military model. The manufacturer noted this as a red flag after she insisted on the military models over the cheaper commercial ones. The investigation found that Ge planned to resell the ships to the Chinese Navy.[164]

Yang was instructed to list her customer as the Hong Kong-based United Vision Limited because "American manufacturers would be more likely to sell to an entity in Hong Kong rather than one in mainland China." To pay for the equipment, Ge used another front company in Hong Kong, Belt Consulting Company Limited, to wire the payment to the engine producer. At the time when the plan was foiled by investigation services, Ge had also coordinated for a representative to go to Hong Kong to transship the parts to mainland China.

Ultimately, after a three year investigation, Ge was sentenced to 42 months in prison for export reporting crimes.

Case Study 13 - Chemical Formula Illegally Exported to China[165]

In 2021, Xiaorong You, a.k.a. Shannon You, was convicted for conspiracy to commit trade secret theft and economic espionage. Shannon was a former employee of the Cola-Cola company in Atlanta and then the Eastman Chemical Company in Kingsport. She worked as the Principal Engineer for Global Research while at Coca-Cola from 2012 to 2017. The technology in question is the chemical formula for a BPA-free coating inside beverage cans. The formula was developed in coordination with several companies including "Akzo-Nobel, BASF, Dow Chemical, PPG, Toyochem, Sherwin Williams and Eastman Chemical Company."

You's intent was to create a company in China producing the same chemical coating. The investigation revealed that You was working for Weihai Jinhong Group and was recipient of funds from the Chinese government. Lastly, You was found to have been

---

[163] https://www.justice.gov/opa/pr/chinese-national-sentenced-more-three-years-federal-prison-attempting-illegally-export

[164] https://www.jacksonville.com/story/news/courts/2021/07/15/feds-chinese-ceo-jacksonville-export-case-wanted-copy-u-s-tech/7944636002/

[165] https://www.justice.gov/opa/pr/chemist-sentenced-stealing-trade-secrets-economic-espionage-and-wire-fraud

the recipient of a Thousand Talents Plan award, further connecting her efforts to PRC state-linked entities.

Case Study 14 - Monsanto Farming Technology Transfer Thwarted[166]

Xiang Haitao was an imaging scientist working for The Climate Corporation in St. Louis. The Climate Corporation is a subsidiary of Monsanto. In his work as an imaging scientist, Xiang developed software that would analyze field data to make predictions and increase farmers' productivity. The algorithm this software relies on was named the Nutrient Optimizer and is the IP of Monsanto and the Climate Corporation.

Xiang left The Climate Corporation in June of 2017 and attempted to board a one-way flight to China the next day. He was met at the airport by federal officials and a search of his belongings revealed that he had with him copies of the Nutrient Optimizer on an electronic device they had confiscated. While they did not arrest him in 2017, they did arrest him upon returning to the US two years later after working for the Chinese Academy of Science's Institute of Soil Science in the interim. In 2022, he was sentenced to prison for conspiring to commit economic espionage.

Case Study 15 - Attempted Theft of GE Turbine Technology[167]

Xiaoqing Zheng worked at General Electric (GE) for 10 years from 2008 to 2018 serving as an engineer specializing in sealing technology. During his tenure at GE, Mr. Zheng had conspired with Zahoxi Zhang, a business partner from the PRC, to steal GE's turbine technology and reproduce said technology in China for profit.

According to the investigation, Zheng stole proprietary files including design models, material specifications, and configuration files that he emailed to Zhang back in the PRC. Supposedly, both Zheng and Zhang were able to leverage the stolen files within Liaoning Tianyu Aviation Technology Co., Ltd. (LTAT) and Nanjing Tianyi Avi Tech Co. Ltd. (NTAT), two Chinese companies that produce components for the turbines in question. Additionally, the investigation purports that the thefts were also intended to be utilized by researchers at PRC national labs and universities. Namely, Shenyang Aerospace University, Shenyang Aerospace research Institute, and Huaihai Institute of Technology had coordinated agreements with Zhang and Zheng.

After a three-year trial and investigation period, Zheng was convicted of conspiracy to commit economic espionage in April of 2022.[168] Though his sentencing date was

---

[166] https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-conspiracy

[167] https://www.justice.gov/opa/pr/former-ge-power-engineer-convicted-conspiracy-commit-economic-espionage

[168] https://www.justice.gov/usao-ndny/pr/former-ge-power-engineer-convicted-conspiracy-commit-economic-espionage-following-four

originally slated for August of 2022, it has been moved to 5 October 2022.[169] Zheng faces up to five million dollars in fines and 15 years in prison.

Case Study 16 – Dual-Use Quantum Telecommunications Network

In 2021 a team at University of Science and Technology of China (USTC) launched a "quantum link" network. The network was developed using technology and equipment from foreign universities and countries. Through this university collaboration, the PRC has developed an 'unhackable' communication network connecting Beijing to Shanghai. To accomplish this, the network uses "over 700 optical fibers on the ground and two ground-to-satellite links."

While the primary goal is to create a link between Beijing and Shanghai, this link accomplishes more than that by linking in other major cities and strategic technology hubs, such as Hefei, Wuxi, and Jinan. If truly 'unhackable' as advertised, the system could easily contribute to the PRC's strategic and military communication systems, well beyond the business-to-business communication between banks that it is currently advertised to support.

This question of unhackability relies on the successful integration of quantum cryptography methods to this system. The satellite utilized for this endeavor is the Miscius satellite developed in 2016 by the same lead professor at USTC that led this project.170 Originally the satellite itself was the vulnerability in the system. The system uses entangled photons to create secret keys used to decrypt the message on the receiving end. Originally, the satellite was a relay point for the message, meaning it would decrypt the message to encrypt it again to retransmit it. To secure the Quantum Link, the satellite itself is no longer needed to decrypt the messages, instead it will simultaneously transmit the keys to two separate ground stations which would be able to detect an error if any interference had occurred.171

The lead researcher even went so far as to say that "we don't need to trust the satellite, so the satellite can be made by anyone- even by your enemy."172 While ominous, this does highlight some of the MCF utility of the satellite which was developed in a partnership with the Institute for Quantum Optics and Quantum Information (IQOQI), Vienna, of the Austrian Academy of Sciences and the satellite does have ground stations

---

169 https://wnyt.com/top-stories/sentencing-date-moved-for-former-ge-engineer-in-economic-espionage-conspiracy-case/

170 https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/

171 https://www.nature.com/articles/s41586-020-2401-y

172 https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/

located in Europe which were developed by IQOQI.[173] This case exemplifies how university collaboration can be used to advance strategic communications with potential dual-use implications.

Case Study 17 – PLA Warships Using German Engine Technology

In 2021, German media published their findings of an investigation claiming German engine technology was being used in Chinese military warships.[174] According to the report, two companies were identified as providing marine diesel engines. These companies were MTU and the French branch of MAN, a Volkswagen subsidiary.

Both companies have reported they are compliant with the dual-use export control regulations and have been involved with China's military in the past. The German media outlet reported that MTU was at least as recently as 2020 supplying engines for Luyang III missile destroyers via a production plant inside China.[175] MTU has also reportedly supplied engines to the Song class of submarines but have stopped. While they claim to have not been contracted by any Chinese defense entity, their 2010 joint venture with the company Tognum had "noted deliveries of 'marine engines for the Chinese navy and coast guard."[176]

The MAN subsidiary, SEMT Pielstick, published on their website its shipment of PA6 engines for frigate generation in China in 2002. They noted that these engines are considered dual-use and did not require an export license.

These instances highlight the need for effective due diligence beyond dual-use controls to prevent risks to the company beyond legality, such as reputational risks. These also pose potential national security risks as companies aid, willingly or unknowingly, to the advancement of China's rapidly growing naval fleet.

Case Study 18 – The Sabirov Affair

"The sanctions they applied on myself, on my companies and on my friends are absolutely unfair, absolutely fake and absolutely wrong" 48-year-old Ilias Sabirov told Reuters after allegedly selling radiation hardened chips to Russia without a license.[177] Radiation hardened chips, which require an export license due to their military uses, are one of the more sought-after items by would-be Russian export busters. Russian

---

[173] https://www.aerospace-technology.com/projects/micius-quantum-communication-satellite/

[174] https://www.theweek.in/news/world/2021/11/07/german-engines-powering-china-warships-eu-arms-ban-torpedoed-by-dual-use-tech.html

[175] https://www.dw.com/en/german-engine-technology-found-in-chinese-warships-report/a-59740301

[176] Ibid.

[177] Special Report: How military technology reaches Russia in breach of U.S. export controls | Reuters

Vice Premier Yuri Borisov, who oversees Russia's defense base for the Kremlin, has said that Moscow was able to produce everything it needed for space flight and rocketry domestically during the Soviet period – but after Perestroika, Russia became ever more reliant on Western components. After 2014, Borisov says "radiation hardened [devices] first and foremost" became difficult to acquire.[178] Sabirov saw this as a business opportunity when he began shipping the devices to Russia in 2015.[179]

Allegedly, Sabirov owned a business in Moscow and therefore could not directly import radiation hardened electronics from the United States. However, the chips could be shipped to Bulgaria. Sabirov allegedly conspired with two Bulgarian businessmen and a Texas company where the Bulgarian company would act as an intermediary.[180] The Texas company sold radiation hardened chips to the Bulgarian intermediary and falsely wrote on the end-user agreement that the Bulgarian company, rather than Sabirov's Moscow business, was the end user.[181]

Case Study 19 – The Brazhnikov Affair

Alexander Brazhnikov Sr. was indicted after he allegedly moved an estimated $65 million in electronics from the United States to the Russian Federation from 2008 to 2014.[182] His customers allegedly included the Russian military, internal security services,[183] and VNIIEF,[184] the latter of which is one of Russia's most important nuclear weapons entities. Operating pre-Crimea annexation in an era of less scrutiny, the scheme was set up in a relatively simple manner. Brazhnikov collected requests for electronics from Russian security entities and transmitted the requests to his son in New Jersey, who pled guilty to illegally smuggling dual-use components to Russia's defense industrial complex and nuclear sites as part of the case.[185] Mr. Brazhnikov Sr. allegedly also sometimes sent the requests to the electronics providers themselves. His son in New Jersey bought the electronics and then sent them to his father in Russia. Mr. Brazhnikov's son only had to lie on the documents about the true end user and lie about the value to avoid scrutiny.[186]

---

[178] https://lenta.ru/news/2022/05/26/thebest/

[179] https://www.justice.gov/usao-wdtx/pr/international-trio-indicted-austin-illegal-exports-russia

[180] ibid

[181] ibid

[182] https://www.federalregister.gov/documents/2021/03/11/2021-05022/in-the-matter-of-alexander-brazhnikov-jr-respondent-final-decision-and-order

[183] https://www.justice.gov/usao-nj/pr/owner-russian-importexport-company-charged-evading-us-export-controls-smuggling-sensitive

[184] ibid

[185] https://www.federalregister.gov/documents/2021/03/11/2021-05022/in-the-matter-of-alexander-brazhnikov-jr-respondent-final-decision-and-order

[186] https://www.justice.gov/usao-nj/pr/owner-russian-importexport-company-charged-evading-us-export-controls-smuggling-sensitive

According to U.S. officials, Mr. Brazhnikov Sr. allegedly created a series of companies in Moscow whose purpose was to act as a false end user. Mr. Brazhnikov Sr.'s alleged true customers, Russia's military, security service and nuclear complex, paid through a series of bank accounts[187] in the British Virgin Islands, Latvia, Panama, Marshal Islands, UAE, U.K. and other secretive bank havens. Profits from the scheme could also be sent back to Mr. Brazhnikov's son in New Jersey with less suspicion that way. The sensitive technologies included: power detectors; fast-settling logarithmic detectors; miniature power relay equipment; thermistors for overload protection; high speed high output current voltage feedback amplifiers; and oscillator frequency convertors.[188]

Case Study 20 – The Kanaev Affair

Tags for cross linking: Front Companies and Intermediaries; Procurement of components; Misrepresentation of contents/origin

Tsvetan Kanev was less successful than Brazhnikov and his son, as detailed in Case Study 19. Tsvetan Kanev was indicted for violation of the International emergency Economic Powers Act and unlawful smuggling after he attempted to buy clock drivers and other controlled items and send them to Russia without a license. Mr. Kanev's scheme fell apart when an attempt by Mr. Kanev to buy radiation hardened circuits from a U.S. supplier failed.[189] Mr. Kanev claimed the circuits were for the Bulgarian Academy of Sciences. However, the American supplier of radiation hardened chips tipped off the U.S. government to the attempt. Mr. Kanev ultimately explained his failed scheme to government informants.[190]

In the scheme, Mr. Kanev was to transship the components to Bulgaria first, and then transship them to Russia via Finland. Finland has historically been a transshipment point of interest given its friendly relations with the West with easy access via land and water to Russia's second city, Saint Petersburg. Mr. Kanev was to use falsified end user agreements in combination with multiple transshipment points.[191]

Case Study 21 – The Baryseff Affair

Tags for cross linking; Front Companies and Intermediaries; Procurement of components; Misrepresentation of contents/origin

---

[187] https://www.justice.gov/usao-nj/pr/owner-russian-importexport-company-charged-evading-us-export-controls-smuggling-sensitive

[188] ibid

[189] https://www.justice.gov/usao-co/pr/bulgarian-national-sentenced-federal-prison-illegal-exports-russian-military-and-space

[190] https://www.nbc11news.com/2021/05/24/bulgarian-national-sentenced-to-federal-prison-for-illegal-exports/

[191] ibid

The Barysheff case involved a naturalized U.S. citizen in Brooklyn and two Russian nationals who were arrested in Denver as part of an alleged scheme to illegally ship microelectronics to the Russian Federation. Barysheff ran a series of locations in New York which served as front companies[192] in the scheme. Barysheff's companies in New York allegedly provided false end user certificates presenting themselves as the user of the electronics, when in actuality, the electronics were shipped to Finland and then on to Russia without a license. Barysheff's companies lied to the Commerce Department about the contents[193] of packages it was sending out of the country. This tactic is used by smugglers and export license violators alike because it plays on the fact that customs officials at ports cannot check every package, and if they do conduct a check, most port officials do not have the technical knowledge to identify many dual use goods.[194]

According to U.S. officials, Barysheff's network transshipped the goods to Finland.[195] Finland has been a popular transshipment point for dual use goods into Russia since the Cold War.[196] Easy water and land access from Finland's main ports to Russia's second city of Saint Petersburg makes the route convenient. Finland's role as a neutral country (until recently) makes it a less suspicious destination than Russia proper.

Case Study 22 - The Flider Affair

Tags for cross linking: Procurement of components; Misrepresentation of contents/origin;

Pavel Flider is a Russian émigré and naturalized American citizen who allegedly used his California company Trident International to transship advanced electronics to the Russian Federation. According to court documents, Flider did this using a series of fronts located in Estonia and Finland. The scheme was caught when U.S. customs officials intercepted an outgoing shipment at the San Francisco airport[197] containing 15 Field Programmable Gate Arrays from the American (FPGA) company Xilinx. Xilinx's Field Programmable Gate Arrays are the Spartan series.[198] The Xilinx Spartan series of products includes a programmable semiconductor that has repeatedly been found inside Russian military drones in Ukraine for years. Flider's network appears to have

---

[192] https://www.justice.gov/usao-edny/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export
[193] https://www.justice.gov/usao-edny/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export
[194] https://www.justice.gov/usao-edny/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export
[195] https://www.justice.gov/usao-edny/pr/brooklyn-resident-and-two-russian-nationals-arrested-connection-scheme-illegally-export
[196] https://direct.mit.edu/jcws/article-abstract/21/4/150/13820/The-Northern-Front-in-the-Technological-Cold-War?redirectedFrom=fulltext
[197] https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/1213-trident-tdo/file
[198] https://archive.ph/z0dWB

sent at least hundreds of the devices to Russia based on seizure data published by American investigators.[199]

Flider allegedly sent the packages out of the country with false labeling. The high-end semiconductors used in Russian military drones seized by U.S. customs for example were labeled as "power supplies".[200] The equipment first went to an Estonian freight forwarder of whom Trident was their only client. The shipments then went through Finland, before being handed to a Saint Petersburg company for distribution amongst Russia's defense industrial base.[201] Money was sent back via a series of bank accounts to mask the source of the funds.[202]

Case Study 23 – The ARC Electronics Network

Tags for cross linking: Aerospace; Front Companies and Intermediaries; Procurement of components; Misrepresentation of contents/origin

ARC Electronics and the Fishenko network is one of the best documented examples of dual-use export busting to the Russian Federation. Alexander Fishenko, as indicted by the US Department of Justice, ran ARC Electronics in Texas and supplied Russia's military and security services with high-value microelelctronics.[203] For years, Fishenko's network was able to conduct this scheme through a combination of falsifying end-users, not applying for required licenses, and lying about the contents of the packages his network was exporting from the United States to the Russian Federation.[204] Fishenko's network sold not only items on the dual use list, but also items on the munitions list. One of the primary points of disembarkation was JFK airport in New York. The shipments then went through Finnish intermediaries to a front company in Saint Petersburg for eventual distribution to Russian defense contractors and entities.[205]

Correspondence between Fishenko and his customers reveals insights as to why the Russian military and security services go through all the risk of acquiring American-made products. According to one of his interlocutors, the Russian military end-users procured American-made products because they "figured out that the Chinese… supply

---

[199] https://www.documentcloud.org/documents/3520133-FLIDER-TRIDENT-COURT-DOCS%20and%20https:/www.govinfo.gov/content/pkg/FR-2018-10-02/pdf/2018-21446.pdf
[200] https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/1213-trident-tdo/file
[201] ibid
[202] ibid
[203] https://www.justice.gov/opa/pr/russian-agent-sentenced-10-years-acting-unregistered-russian-government-agent-and-leading
[204] https://www.wired.com/images_blogs/dangerroom/2012/10/indictment.pdf
[205] https://www.wired.com/images_blogs/dangerroom/2012/10/indictment.pdf

crap". This preference for Western over Chinese goods is seen throughout case studies and research by CNS.[206]

Case Study 24 – Codename Firebird

Reserved

Case Study 25 – Putin's Bunker

Reserved

Case Study 26 - German Production Equipment for Russia's Defense Industrial Base

Reserved

Case Study 27 - German Robots for Russian Weapons Labs

Reserved

Case Study 28 – American, French and Dutch technology for Russia's Quantum Dreams

Reserved

Case Study 29 – Powered by...

Reserved

Case Study 30 – The Singapore Connection

A Russian Orlan-10 drone captured by Ukrainian troops contained a Xilinx brand semiconductor in the drone's targeting system. The image taken of the drone was clear enough to show the product line and other identifying markers such as its place of manufacture. Using trade data, CNS researchers gathered import data on all imports of Xilinx brand products to Russia from the time period of January 2017 to October 2021. From there, CNS researchers keyword searched the import data for the product code "Spartan-6". There were 10 results. Two of those results led to a wholesaler in St. Petersburg, the city where the drone's manufacturer is located. [207]

---

[206] ibid

[207] Internal CNS Report. CNS cross-referenced detailed Russian customs documents with public tax records of electronic wholesalers in the vicinity of the Orlan-10 manufacturer

The importer, an electronics wholesaler in St. Petersburg EFO Corporate, is located at 9 Mendeleevskaya Street in Saint Petersburg's Kalinin District. The trade declarations in possession of CNS name this same address as the custom broker's address for both the May 2019 and October 2019 deliveries. The manufacturer of the Orlan-10 drone, the Special Technology Center, is also located in Saint Petersburg's Kalinin District, with Google maps putting the estimated drive time between 9 Mendeleevskaya and its office as 13-15 minutes. Given the reliability of Russia's pre-February 24th data, and the limited number of Spartan-6 chips that were exported to Russia, it is highly likely this was a means of acquisition.[208]

The providers of the Spartan-6 Xilinx chip were listed as "Not Available" and "Astro Express Logistics," a Singapore-based freight forwarder in trade data held by CNS. It is imperative that companies recognize red flags such as freight forwarders and verify the ultimate end users of their products.[209]

Case Study 31 – Poisons for Putin

Reserved

Case Study 32 – The French Connection

Reserved

[208] ibid
[209] ibid

Annex 2: Further resources and guidance

Sanctions and restricted party lists

There are many known entities of concern in China and Russia which are involved in weapons of mass destruction, military, and other end uses of concern. There are no UN sanctions in place given that both countries are veto-wielding members of the UN security council. However, other individual countries have identified entities of concern in their national sanctions lists. This includes the sanctions lists of the US, EU and Japan. The basis of adding entities of concern to such lists varies from country to country and the inclusion of an entity on such a unilateral sanctions list is not binding to entities operating outside the relevant jurisdiction. Nonetheless, the inclusion of any entity in such a list is a clear indicator that there is a risk associated with commerce with the entity. Companies should thus use such lists as part of a risk management approach. This implies screening customers and partners against such lists and taking a considered approach about what to do when a potential customer or partner is listed. The inclusion of an entity on such a list may be grounds to assert that a company 'knew or had reason to know' that there was a military or WMD related concern with the party. It may be beneficial or necessary to refer the case to relevant national authority for guidance on whether a weapons of mass destruction or military end use control would be applied.

- EU consolidated sanctions list
- US non-SDN list
- US SDN list
- US entity list
- UK sanctions list
- Australian sanctions list
- Canada sanctions list
- Japanese METI List

Media and NGO resources

As with lists of sanctioned entities, you should know if a customer on partner on a dataset of entities of concern published by a media outlet or an NGO. Inclusion of an entity in such a list does not necessarily mean that business should not be conducted. Instead, it is a potential indicator of risk that should be systematically assessed and managed. It is possible that inclusion of an entity on such a database would be grounds for you to know or have reason to know of a WMD or military related end use in a transaction, although it is perhaps less likely than if the entity was listed by a government or international organizations.

- ASPI Database of Chinese Military Linked Universities
- Wisconsin Project Risk Report

- NTI country profiles

Due Diligence Tools and Techniques

Annex 3: Advanced Web Searches

Major web search engines such as google generally offer advanced search tools that can be helpful in uncovering due diligence related information.

Google Site Search

Googling the following will identify any pages on the site mentioning the exact term, export control. This approach can be taken for any website and with any keyword. It can also be used in combination with Boolean operators (see below).

```
site:https://nonproliferation.org "export control"
```

Domain Search

Similar to site search, Google allows you to search a country's entire internet domain (i.e. .ru in the case of Russia) to identify keywords. Domain searches are generally best undertaken in the country's own language.

```
site:.ru "export control"
```

Boolean Search

Some web search engines such as Google allow the use of Boolean operators. The following returns results that mention China.

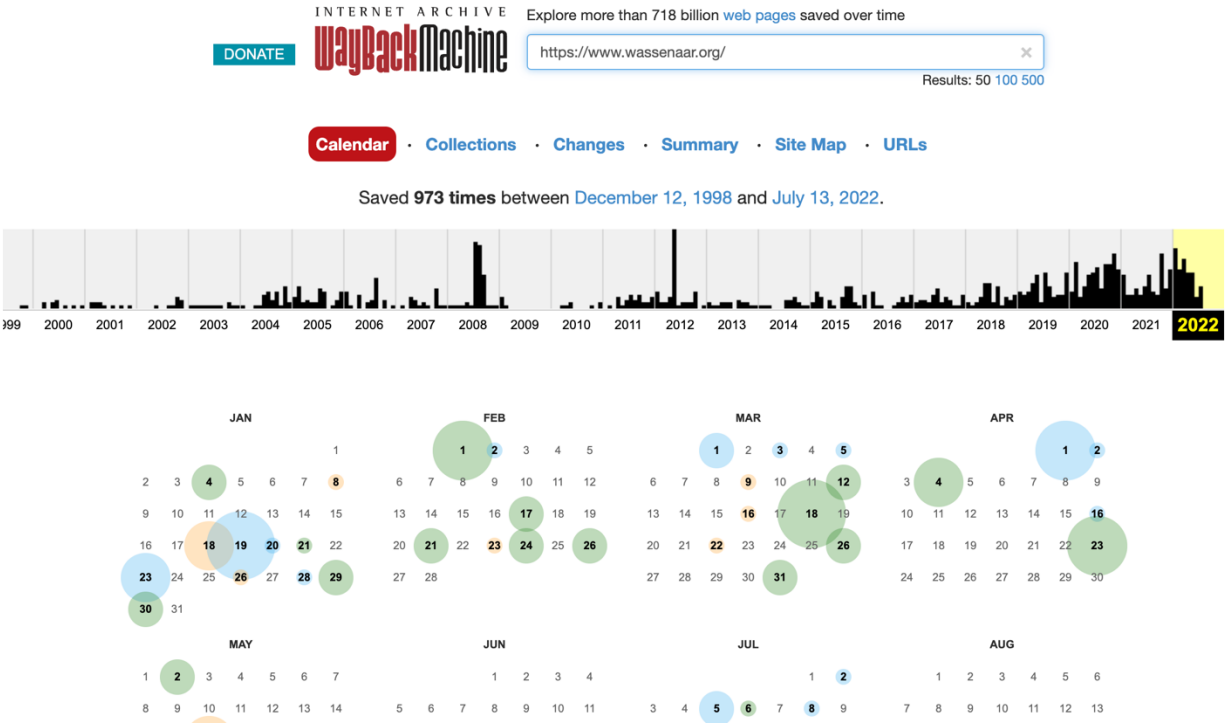
```
site:.ru "export control" AND China
```

The following returns results that do not mention China.

```
site:.ru "export control" -China
```

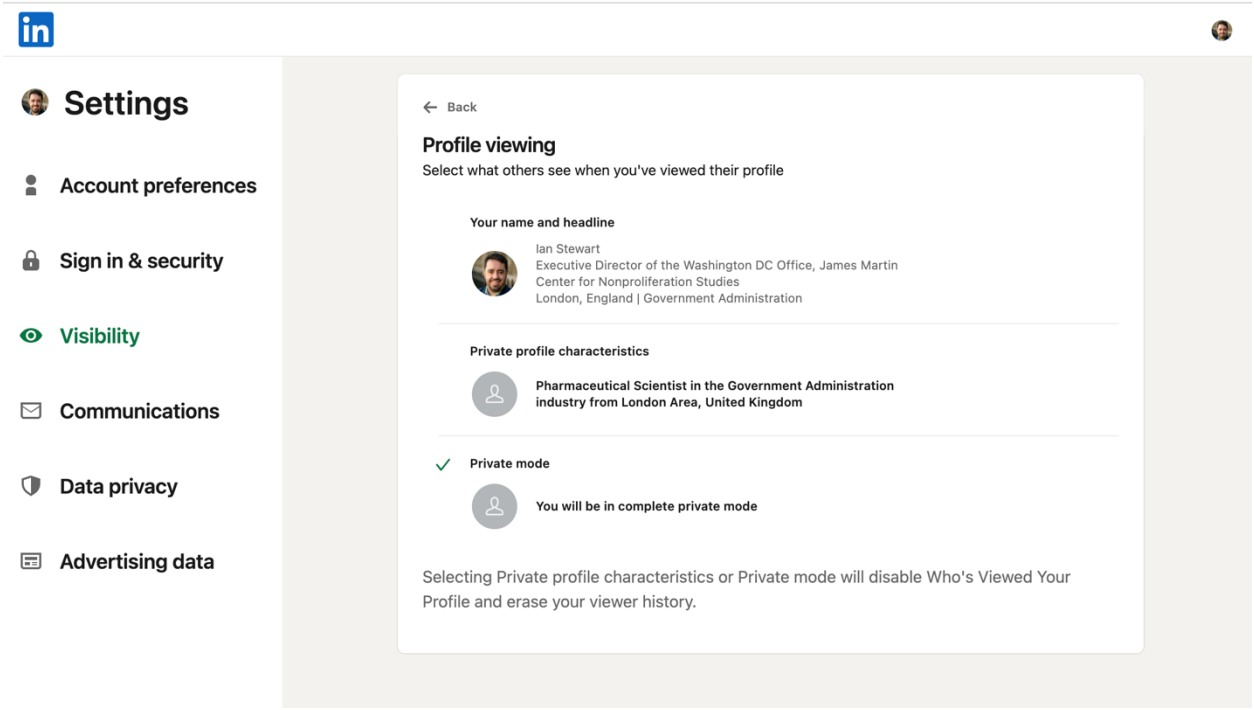
Way Back Machine

It is often useful to be able to refer to older versions of a website particularly in the context that information cab be removed from websites to obfuscate a company's role. A useful tool for this is the Way Back Machine (https://web.archive.org/), which is a project of the Internet Archive. Over the years, the Way Back Machine has taken copies of many websites. Although it is less likely that the Way Back Machine will have captured clones for obscure websites, it is worth checking whether the platform has stored previous copies of any site of interest.



Using LinkedIn Anonymously

Linkedin can be a useful due diligence tool as it contains relevant information on individuals including their employers, employment history, education and publications. When looking up profiles on Linkedin for due diligence purposes, more information is available if the searcher has a Linkedin account. At the same time, it can be desirable to search anonymously so that the target of the search does not identify the individual conducting the due diligence. In these circumstances it can be useful to enable Linkedin's anonymous 'profile viewing' option, as shown below. This allows the searcher to view profiles without revealing their identity.



Annex 5: Red Flags broken down by technology transfer means and technology sector

Red Flag	Relevant to Sector	Relevant to (state / companies)	How to monitor	Links to case studies
Chinese entities offer above market salary to run	Semiconductor,	States		

production lines in China				
Military-linked university in China proposes joint research, cooperation or funding.	All	States, Universities	Incorporate ASPI database into screening system	
Chinese partner is linked to Chinese government or Chinese strategic plans	All	States, Universities, Companies	Chinese entity has language on military civil fusion on its website. Chinese company has a communist party section on its website	
Russian-run company outside of Russia procuring goods to ship to Russia	All	States, Companies	As part of due diligence, establish whether the company is Russian run and establish whether the company has a pattern of shipping goods and material to Russia.	Novichock networks, Sabirov Case, Brazhnikov Case, Kanaev Case, Barysheff Case, Flider Case, Fishenko Case
Small general wholesalers in Russia, particularly in Moscow	All, but semiconductors and microelectronics relevant to aerospace or drones especially	Companies	As part of due diligence, check whether or not the company is involved in the defense trade or	The wholesalers supplying the Novichock networks. The various wholesalers who openly

			subcontracts. This is usually advertised on their website	deal with the Russian defense industry and security services.
Your subsidiary is doing business with the Russian military or intelligence services	All	Companies	Oversight of company activities in Russia	Case 9, Case 10
University is affiliated with Russia's defense manufacturing base or security services	Aerospace, Telecomms	Companies	Know your customer	Case 8, Case 10, Case 11

www.nonproliferation.org/dc