Working Group Paper #7

IT & Supporting Technologies: Recommendations for Sanctions against the Russian Federation

International Working Group on Russian Sanctions

November 2, 2022

https://fsi.stanford.edu/working-group-sanctions

Introduction

The International Working Group on Russian Sanctions[1] aims to provide expertise and experience to governments and companies around the world by assisting with the formulation of sanctions proposals that will increase the cost to Russia of invading Ukraine and that will support democratic Ukraine in the defence of its territorial integrity and national sovereignty. Our working group is comprised of independent experts from many countries, but coordinates and consults with the Government of Ukraine and those governments imposing sanctions. This consultation process helps to inform our views, but our members express independently held opinions and do not take direction from or act at the behest of the government of Ukraine or any other person or entity. This publication is a follow-up to our first Action Plan and previous working papers on energy, finance, individual sanctions, and designating Russia as a State Sponsor of Terrorism, and confiscating Russian Central Bank reserves, all of which have been informed by additional memos and publications from our working group members on our website.[2]

Executive Summary

Foreign information and communications technology, microelectronics, related hardware and machinery, and intellectual property (hereafter "IT") currently underpin Russia's military, military-industrial complex, and government more generally.[3] Compared to other nations, Russia has largely been a laggard in IT compared to other nations and therefore relies on foreign IT to command and control its military, fire its weapons, perform reconnaissance, control the information space, attack Ukrainian cyber and civilian infrastructure, and protect its own infrastructure. Foreign technology used by Russia includes everything from advanced email servers, network management capabilities, smart devices, software-as-a-service applications, crypto and blockchain services, and video streaming all the way to Computer Aided Design and Manufacturing (CAD/CAM) and Building Information Modelling (BIM) engineering design, manufacturing, and simulation software, as well as robotic components and device controllers.

A recent report suggests that approximately 38% of IT and 63% of electronics imports into Russia come from the European Union, United Kingdom, and the United States alone.[4] Since invading Ukraine on February 24, 2022, the Russian government has tried to requisition foreign IT and microelectronics components from consumer products for use by its military. As a result, there is no clear distinction between IT goods and services delivered to Russia for "civilian" use and those that are being repurposed for military

[1] All members of this working group participate in their private capacities, but we have consulted with numerous government officials, including with the Government of Ukraine.

[2] Similar to other papers produced by this working group, our aim in this paper was not to produce a consensus document, but instead to provide a menu of possible additional measures to be considered by governments, multilateral institutions, and private actors. The implications of every sanction have not been thoroughly analysed, and not everyone necessarily agrees with every specific sanction or action proposed.

[3] Daniel Perez Fernandez, "Made in Russia: Making sense of the Kremlin's IT import substitution program," Georgia Tech School of Public Policy Internet Governance Project, October 19, 2021. https://www.internetgovernance.org/2021/10/19/made-in-russia-making-sense-of-the-kremlins-ict-import-substitution-program/

[4] Scott Marcus, Nicolas Poitiers, Monika Grzegorczyk, and Pauline Weil, "The decoupling of Russia: high-tech goods and components," Bruegel Blog, March 28, 2022, https://www.bruegel.org/blog-post/decoupling-russia-high-tech-goods-and-components

use against Ukraine. Foreign IT is enabling Russia's war machine and its propaganda machine. That must be disrupted and ultimately stopped.

The sale and maintenance of IT technology and related capabilities to any entity within Russia that enables the Russian invasion of Ukraine, whether directly or indirectly, should cease immediately. This document provides an analysis of the areas that should be immediately sanctioned, how to do so, and how the corresponding technologies support Russia's war infrastructure and military operations in Ukraine.

This paper recommends that concerned governments and IT companies take immediate measures to:

1. Block access to IT that supports Russia's war machine and its use against Ukraine.

2. Block access to IT that enables Russia's information and cyber warfare against Ukraine and others.

3. Block access to IT that enables the Russian government's ability to isolate its population from the consequences of Russia's actions.

Democratic governments and IT companies located within them must take precise actions that aim to cripple the Russian war machine in Ukraine, but do not damage to Ukrainian government entities, the Ukrainian private sector, Ukrainian civil society, or Russian actors using technology to effectively oppose Putin's war. Western social media companies continue to play a critical and positive role in sustaining Russian civil society and political opposition. YouTube, for instance, provides indispensable support to Russian independent media. The task of preserving the good that these companies do while restricting the harm is difficult, but not impossible.

This document is organised as follows:

Part I outlines our objectives in sanctioning Russia's access to IT.

Part II details our recommendations and their expected outcomes.

Part III summarises the need for robust IT sanctions against Russia, emphasising that there is no longer a "dual-use" distinction in IT, as foreign IT plays essential roles in Russia's war machine and information machine. Consequently, there is a need to increase pressure on key Russian sectors to prevent them their facilitation of Russia's war in Ukraine and its information operations against other countries.

Part IV lists the IT that should be subject to sanctions and re-export and re-sale prohibitions.

Part I. The Purpose of IT Sanctions

Russia's attempted imperialist conquest in Ukraine is the most technologically enabled war that the world has ever seen. Information technology (IT) allows both sides to scale real-time information-gathering efforts via unmanned aerial vehicles (UAV) and satellite imagery; to interpret imagery with identity-matching technologies and computer-vision capabilities; to merge social, geo-, and operational datasets; to track and target individuals; to attack digital infrastructure of social, industrial, and government services; to wage broad information wars and targeted propaganda efforts; to guide missiles, flight paths, and military decision-making; and to funnel funds to Russians fighting in Ukraine, among other functions.

Central to what this paper calls Russia's "war machine" and "information machine," IT is defined here as information and communications technologies, microelectronic components and devices, and their attendant intellectual property. A detailed list of IT that should be sanctioned can be found in **Part IV** of this paper.

Since Russia's first invasion of Ukraine in 2014, Russian President Vladimir Putin and his regime have attempted to decouple Russia's economy from the West. This strategy that has negatively impacted Russia's economic, political, and technological strength and the wellbeing and prosperity of average Russians. Despite these aims, Putin has failed to make the Russian economy independent of Western IT.[5] As a result, robust IT sanctions will severely hamper both Russia's war machine in its operations against Ukraine and Russia's ability to use its information machine against Ukraine, the West, and the Russian population.

This document provides a series of recommendations that, taken together and implemented completely, would accomplish the following objectives:

- Quickly and severely limit Russia's ability to continue its war efforts in Ukraine;
- Decrease the effectiveness of Russian information operations and war propaganda within and beyond Russia;
- Increase Russian military vulnerability to Ukrainian counterattacks; and
- Facilitate the liberation of occupied Ukrainian territories.

Beyond their immediate impact, these sanctions would further reduce Russian economic productivity, which in turn would degrade the long-term output of Russia's military industrial complex. For sanctions to be effective, it must be difficult for Russia to fill the gap with alternative suppliers. Therefore, we also identify means to prevent sanctions-evasion by third parties.

[5] Stanislav Tkachenko, "The Political Economy of Russian Information & Communication Technologies", PONARS Eurasia Policy Memo No. 533, June 2018. https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm533_Tkachenko_June2018.pdf

Part II. Recommended Measures

It is necessary to block the ability of the Russian government and its partners to use or source IT that contains software, firmware, and components that were manufactured by, or contain intellectual property from, any sanctioning nation. This includes IT developed in non-sanctioning nations that entails *de facto* the re-export or re-sale of IT from sanctioning nations. In other words, sanctioning nations should prevent Russia's ability to evade sanctions by importing from non-sanctioning nations IT which incorporates any hardware, feature, or library, or communicates with any device/service, storage facility, or network switch, that is owned, controlled, operated, or managed by a legal person under the jurisdiction of a sanctioning nation.

1. Stop Military Use of Technology

We recommend the removal of existing resources and access to digital services, accounts, and data (computational resources, storage, API's, infrastructure services), a deactivation of hardware, firmware, software, and services used on local servers within Russia, a block on access to support services or updates, a block on any auxiliary features of technology products or services that require access to resources located in sanctioning nations, or that is owned/managed by legal persons under the jurisdiction of sanctioning nations, unless such technology and services are deemed to not have any dual-use potential by sanctioning governments, or in specific cases where the likely humanitarian costs or debilitating costs to Russian civil society require a more sophisticated and targeted approach.

These sanctions must apply to any of the following that relate to products for, services for, or dealings with Russian and non-Russian entities operating in Russia:

- Physical goods shipped to Russia;
- Digital goods, services, and intellectual property, whether transferred physically or virtually, used remotely or on premises, activated by licence or updated;
- Technology "consulting" services;
- Data/code storage/management;
- Electronic communication, documentation, and digital assets; and
- Industrial machinery, components, and inputs.

We also recommend that sanctioning-nation companies not be allowed to divest their technology assets in Russia as an easy way out of sanctions compliance. Government supervision is required on a case-by-case basis. Such divesting behaviour would achieve exactly the opposite of the desired impact. For example, a company with a data centre in Russia should not be permitted to simply divest of the capability to a Russian entity, since this action would increase the technology resources available to the Russian government, potentially providing them with thousands of state-of-the-art microchips, software licenses, and other critical technology of a dual-purpose. This scenario is true not only in IT-specific examples, but also the case with manufacturing facilities or knowledge-driven businesses.

To better achieve these ends, we recommend the introduction of new requirements in terms of sales documentation and Know-Your-Customer procedures, in order to ensure all companies providing IT capabilities to Russia directly and indirectly can be monitored and evolve as needed.

2. Combat Weaponisation of Internet Platforms

We recommend that sanctioning nations adopt regulations that combat Russia's weaponisation of internet platforms through its "attention-trapping" and bot-networks that leverage the incentive structures of IT platforms against the best interests of the global public. Such techniques include effective disinformation campaigns and the silencing of critical voices.

Sanctioning governments should make all social and content-sharing platforms subject to:

- User-verification protocols for all accounts whose content interacts with a large number of other users;
- Shared responsibility for highly consumed content that is similar to broadcast and press requirements (e.g., Ofcom in the UK); and
- Requirements to resolve complaints relating to blocked or limited accounts within strict time periods, including transparency and independent review for users who wish to appeal those actions.

3. Require Deemed Export Licensing

We recommend that sanctioning nations adopt regulations that require Russian nationals to be subject to "deemed export licensing" requirements in order to interface with IT that is important to Russia's war efforts or that is useful in thwarting Russia's war ambitions. These measures would be akin to Chinese nationals working in the United States and obtaining deemed export licences prior to working with certain semiconductor IP, processing, and manufacturing equipment. We recommend that Russia-based IT workers of sanctioning nation entities be subject to similar requirements.

4. Ensure Enforcement of Sanctions

We recommend the creation of a joint agency, e.g., an IT Action Task Force, to manage and monitor Russia's access and use of sanctioned technology. It should be empowered to hold accountable legal persons under member-states' jurisdiction whose products continue to be used in Russia's war efforts. Such an organisation could monitor Russia's efforts to import controlled technology from non-sanctioning nations. The Financial Action Task Force or the Wassenaar Arrangement could serve as a model for such a collaborative agency.

5. Promote Access to Information about the War

We recommend that any sanctioning-nation consumer technology platforms that continue to be available in Russia (e.g., news platforms, video networks, social media, online games, adult websites) commit greater attention and resources to providing end-users in Russia with access to information on the situation in Ukraine. We recommend the funding of an independent, international, multilateral fact-checking entity – existing or new – that would be responsible for the daily selection of representative evidence-supported statements and resources regarding the war. Advertising-type interactions, pop-ups, interstitial windows requiring scrolling, or a wide array of other web-based behavioural mechanisms could help bring the war to Russian web users' attention.

This recommendation is targeted not only at large content sharing websites such as YouTube, but also other user-facing web portals that are active in Russia. We further believe it is important for these platforms to be transparent with respect to the consumption patterns of users on their platform on a country-by-country basis, thus providing benchmark information on the reach of pro-Kremlin propaganda compared to more balanced sources of information. Such reports must be published regularly and contain sufficient details for scientists and policymakers to answer questions relating to the relative benefits and drawbacks of each platform's operations in Russia and around the world.

6. Assess Anticipated Outcomes

Through the foregoing objectives and recommendations, we anticipate the following outcomes:

1. Degrade the ability of the Russian military to leverage IT from sanctioning nations in order to attack Ukraine. This includes, among other things:
   - The ability to scramble or spoof GPS/AIS signals;
   - The reliability and quality of telecommunications;
   - The ability to perform reconnaissance or guide weapons;
   - The ability to carry out radar blocking;
   - The ability to hack or otherwise compromise UAVs;
   - The ability to identify electromagnetic signatures of equipment;
   - The ability to train and equip troops;
   - The ability to effectively command and control the military;
   - The ability to build, connect, or otherwise manufacture items of a military or dual-purpose nature; and
   - The ability to build and maintain supply, logistics, and supporting operations in all theatres of the war.

2. Degrade the ability of the Russian government to perform cyberattacks against social and industrial digital infrastructure in Ukraine and beyond.

3. Degrade Russia's physical and cyber operations in the space domain, including degrading the ability of Russia to carry out Direct Ascent Anti-Satellite Weapons Testing (DA-ASAT) or other offensive kinetic anti-satellite attacks, as well as jamming and cyber-attacks on commercial and military space assets.

4. Shift Russia’s allocation of cyber resources from offence to defence through the denial of IT from sanctioning nations. Force Russia to allocate more personnel and associated resources from offensive cyber actions against Ukraine to plugging gaps in Russia’s defensive capabilities.

5. Degrade the ability of the Russian government to spread disinformation through “information warfare” and propaganda strategies both within and beyond Russia.

6. Degrade the ability of the Russian government to isolate Russia’s tech sector from the economic and social effects of the war in Ukraine, to increase the costs of continuing to supply the Russian government’s war and information machines.

7. Limit sanctions evasion through creation and enforcement of re-export and re-sale bans on sanctioning nations’ IT.

Part III. The Need for Robust IT Sanctions Against Russia

1. There Is Little Distinction between Civilian and Military IT

For all intents and purposes, there now is no clear distinction between civilian and military use of IT in Russia. Any foreign IT or industrial machinery/inputs imported into Russia may eventually be used to further Russia's war aims.[6] This includes the repurposing of components from consumer goods (phones, computers, Internet-of-Things [IoT] devices, etc.) for military ends. Due to the success of recent restrictions on semiconductor sales to Russia, the Kremlin is finding it increasingly difficult to repair equipment and produce newer weapons systems with foreign onboard components, including drones and other key resources. The Russian military-industrial complex has resorted to using microchips and other components from consumer electronics in order to produce and repair some types of weapons systems. Consumer digital cameras appear in its flagship drones. At this point, any foreign technology- or knowledge-transfer or digital infrastructure may be used to sustain Russia's military activity in Ukraine.

The Russian government and military rely also on foreign off-the-shelf corporate operations software for communications, analysis, human resources, logistics, and other functions that form the backbone of current offensive military and information operations against Ukraine and other countries. To a large extent, the Russian military relies on foreign commercial hardware and software to manage logistics, support field operations, manufacture equipment, communicate with recruiting offices across the country, plan and carry out training, and coordinate with the military-industrial complex.[7] To the extent that it relies on technology running via smartphones and similar retail end-user devices, the Russian military's deadly operations in Ukraine depends on a panoply of foreign IT services present on foreign devices. Foreign corporations can disable key services on these devices that render them largely unusable for military purposes.

Since Russia invaded Ukraine in February 2022, most services from major foreign technology companies continue to be available to existing clients within Russia. Russian devices continue to receive updates/software patches and thus be exploited for battlefield uses by the Russian government. Foreign components are currently being "found in Russian *materiel* used in the war on Ukraine. Many of these items were manufactured after 2014, when the war in eastern Ukraine first began and the European Union and United States imposed an initial set of sanctions on the Russian Federation."[8]

Additionally, Computer Aided Design and Manufacturing (CAD/CAM) and Building Information Modelling (BIM) software packages play a vital role in the development of a wide range of modern

[6] James Byrne et al, Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine. RUSI, August 2022, https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[7] James Byrne et al, Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine. RUSI, August 2022, https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

[8] Conflict Armament Research, "Component commonalities in advanced Russian weapon systems,"
Ukraine Field Dispatch, September 2022,
https://storymaps.arcgis.com/stories/239f756e2e6b49a5bec78f5c5248bf3d

technology systems. CAD/CAM/BIM engineering software giants like France's Dassault Systèmes (maker of the SOLIDWORKS), Boston-based PTC (maker of PTC Creo), and Bay Area-based Autodesk (maker of Autodesk Inventor and Revit) have reported winding down operations in Russia following February's large-scale invasion, although products generally remain available in Russia for existing customers. Global democracies should continue to build out export controls and oversight mechanisms to limit the availability of advanced CAD/CAM/BIM software to Russia, since their capabilities can be used not only to support a well-functioning high-tech sector, but also to advance the project development and manufacturing of advanced offensive, defensive, and logistical-support military components, systems, equipment, and infrastructure.[9] It is therefore imperative that Russia must not access any IT that plays a role, or could substitute for any item that plays a role, in sustaining Russia's war in Ukraine.

2. Foreign IT Continues to Enable Russia's War Machine

Russian munitions, missiles, guidance systems, artillery, defensive weaponry, and a range of heavy equipment, tanks, submersible vessels, etc., all rely on components or manufacturing techniques that are not directly owned by Russia. For example, the DMG Mori Seiki Company is a German-Japanese provider of high-precision manufacturing hardware and software used by Russia for artillery barrels and Kalibr missile components. Such modern manufacturing equipment relies on ongoing service provision (e.g., active fault detection and maintenance services, internet information services, remote operation and diagnostics), and the intervention of foreign expertise and spare parts in order to operate continuously at full capacity. In general, any industrial system or functionality that enables design, operation, manufacturing, testing, quality assurance or logistics relating to dual-use goods and technologies needs to be addressed as part of direct and comprehensive sanctions. This designation would include the operations of companies such as Siemens and Oracle, who provide critical backbone and support systems for Russian industry.

Russia's battlefield communication is enabled by hybrid networks that seamlessly switch between radio, satellite, and local smart network hubs in order to securely transport messages over foreign smartphones and similar devices often running foreign software or software incorporating foreign libraries and capabilities. Hindering Russia's battlefield communication and reconnaissance limits its ability to undertake offensive operations and reduces their success.

Russia's military IT includes internet-enabled consumer devices that depend on foreign IT in several ways. Russian military IT communicates with a range of foreign services in the cloud and relies on foreign operating systems, security or communications libraries and protocols. It includes IoT devices with remote sensing capabilities that can be remotely disabled and software or firmware that relies on regular updates or patches from foreign companies to fix discovered vulnerabilities. Most of this foreign IT is owned, designed, or produced by entities in sanctioning nations.

[9] Benjamin Schmitt, "Don't Stop Now – Tech Sanctions Can Wreck Putin's War Machine," *Center for European Policy Analysis,* July 28, 2022, https://cepa.org/article/dont-stop-now-tech-sanctions-can-wreck-putins-war-machine/

There are situations where Ukraine's military is in close contact with Russian military units during active combat, which raises the concern of inadvertently interfering with Ukrainian military systems when intending to disable and degrade Russian military systems and technology (something the Ukrainian military deals with every day with Starlink's active network nodes). We note that device- and network-based features can be used to understand provenance. We look to features such as the use of Russian networks, sim cards, and communication with services located in clearly Russian-held territories and into Russia itself, in coordination with the Ukrainian military as needed. We highlight the fact that significant network disruptions to military uses do not require a complete removal. Disabling sufficient services clearly associated with Russian military movements and support or logistics networks will effectively disable frontline services. We recommend a measured and intelligent approach but reiterate the primary importance of removing access to the extent feasible.

3. Foreign IT Continues to Enable Russia's Information Machine

Russia's weaponisation of foreign IT extends to both the cyber and physical realms. The Russian government deploys highly skilled IT units to exploit weaknesses in foreign nations' digital infrastructure, often with the aim of inflicting damage on digital and physical infrastructure. Ukraine's financial sector and government services have come under sustained attack for many months, and attacks on US, EU, and UK digital infrastructure have also been attributed to Russian cyber units operating under official guidance. Sanctions should hinder cyber assets and infrastructure underlying Russia's war and propaganda machines, regardless of whether those assets are ultimately owned by the Russian state or Russian non-state actors that support those same aims. Sanctioning nations must reduce Russian state and non-state entities' ability to carry out attacks and compromise the cyber infrastructure, democratic institutions, and information space of Ukraine and sanctioning nations.

Although many sanctioning nations have placed restrictions on the sale of military-related components and supporting systems to Russia, foreign software, services, technical infrastructure, intellectual property, and other less tangible items have not been explicitly covered by sanctions or restrictions beyond a core set of known government-related entities. Companies within sanctioning nations have been largely left to decide whether to continue operating in Russia and how to alter their Russian operations.

As a result, Russian government and non-state actors continue to exert significant influence over public information and opinion in Russia and sanctioning nations. This influence happens both through enabling technology at the network-level, data analysis and Business Intelligence, programming languages (e.g., Matlab, SAS, C#), as well as at the web user platform level. Inside the country, remaining platforms are built on Western technology, and often hosted in data centres controlled by sanctioning nation entities or their technology. Outside the country, the platforms enable the Russian government to reach countries and populations around the world. Social networks, advertising networks, traditional media, and strategically timed propaganda campaigns against key political figures in Ukraine, sanctioning nations, and the Russian opposition form part of a programme to continuously and comprehensively manage public opinion, sow confusion, and warp public messaging to Russia's advantage. Russia can infiltrate and exploit virtually any network that allows people to share content, build communities, buy and sell from each other, and participate in common activities on- and offline. Any technology that allows for Russian dissemination of disinformation and potential large-scale "viral" spreading of propaganda, if it is not to be blocked entirely, needs pre-emptive, transparent processes to minimise the Kremlin's reach (akin to trading breaks in financial markets). This requires changes in how IT platforms structure their services.

To reduce dissemination of disinformation and misinformation from Russian and other malign actors, fundamental regulatory and governance mechanisms need to be enacted. These measures would increase the resilience and responsibility of content platforms to disable manipulation. This would in turn decrease the power of Russian state and non-state actors in promoting their information war against Ukraine and sanctioning nations. Critically, IT companies must credibly commit to reducing content that amplifies and echoes Kremlin narratives. For example, initiatives such as that of the Institute for Strategic Dialogue, benchmarking tendencies of social media platforms to reinforce echo-chambers,[10] should be expanded (and include Russia in the analysis) to aid in the application of sufficient pressure. Advertising networks should be held in violation of sanctions for selling programmatic advertising space to any Russian entity and should be responsible for full ultimate-beneficiary verification.

4. Foreign IT Allows Key Russian Sectors to be Isolated from the War

In the last ten years, Russia has invested heavily in creating an internet infrastructure that can be isolated from the outside world, working closely with sanctioning-nation technology giants to allow certain services to keep operating, while filtering out "undesirable" content. The Kremlin, much like the People's Republic of China, is only interested in retaining foreign technology on its network whose parent companies specifically yield to its demands. Tech companies operating inside Russia still provide valuable support for the flow of independent media and non-Kremlin controlled content. However, conforming to Russian restrictions on their operations can indirectly support Russia's war and information machine.

Over the past five years, the Russian government has significantly ramped up internet traffic monitoring operations, as well as the digital and physical tracking of politically sensitive individuals who may disagree with the Kremlin. This tracking uses in part foreign IT to identify infrastructure vulnerabilities in network equipment in Russia and around the world. Much of the required physical components would be difficult to obtain today due to existing sanctions, but new sanctions are needed to ensure the entire stack of technologies becomes impossible to maintain in the medium term.

Putin's intention to migrate Russia to an isolated centralised and resilient internet infrastructure, or 'splinternet,' aims for complete control of information moving over the network. Such a network would allow the Russian military to threaten global internet infrastructure, such as underwater cabling projects, while limiting the internal repercussions of such acts. It would increase Russia's power to target global information flows, financial markets, energy assets, trade, etc., with impunity. Sanctioning nations should therefore prohibit the use of foreign IT in creating Russia's splinternet and isolating its economy

[10] Institute for Strategic Dialogue, "404 Reliable Information Not Found", Report, August 16, 2022, https://www.isdglobal.org/digital_dispatches/404-reliable-information-not-found/

from the global information ecosystem. Moreover, these recommendations seek to limit Russia's exploitation of Western technology in general and prevent the Russian government from isolating the way the internet works, which, ironically also requires Western technology to be achieved.

At the same time as denying Russia technology directly, we are aware that third parties with viable alternatives (such as China) may attempt to fill the gaps left behind and undermine the intent of sanctions. We strongly urge sanctioning countries to continue to incentivise those countries to not participate in such a land grab and consider the introduction of secondary sanctions should the situation warrant such a step.

Our recommendations also have an economic focus. Technology migration is extremely difficult when faced with the disconnection of existing infrastructure and processes (as it is difficult for Ukrainians to repair energy infrastructure while under attack). It involves not only large costs in equipment and software purchases, but human labour, training, and loss of productivity through restructuring teams and business processes. This money cannot be spent on the destruction of Ukraine.

Since 2012, Putin has sought to break Russia's reliance on foreign technology through growing an indigenous Russian IT sector. This effort has yielded a small tech sector that is lacking in innovation and is not globally competitive. As a result, Russia's tech sector is heavily dependent on government contracts, thereby making the identification of technology channels to the government extremely difficult. Innovative parts of this sector rely on partnerships with foreign companies that transfer knowledge and technologies such as artificial intelligence and machine learning. Increased isolation of this sector from sanctioning-nations technology will decrease its innovation capacity.[11]

The Russian government maintains many of its own technology and software systems in order to secure communications, spoof radar, GPS, and AIS signals, intercept and interfere with radio and satellite systems, filter internet traffic, and perform a variety of signal processing tasks. These systems are often a patchwork of outdated technology packages mixed with modern state-of-the art capabilities. Such systems rely on fragile human knowledge networks in the case of problems. Small perturbations to these systems can have outsized impacts. As such, IT personnel are a critical asset to the Russian government**,** one that is currently directly and indirectly supporting Russia's war on Ukraine.

Almost two million high-skilled Russians work in Russia's tech sector, representing about 5% of Russia's active labour market in 2021. Since February 2022, estimates of tech workers leaving Russia range from 300,000 to 600,000, although their long-term status remains unclear. Many of the workers who have left were working for foreign IT companies as employees or freelancers through platforms such as Fiverr and Upwork. These tech workers generally earn high wages. Sanctioning countries should be doing everything that they can to keep these tech workers from returning to Russia.

Many foreign tech companies still have active operations and employees in Russia, either directly or through subsidiaries. Tech platforms in sanctioning nations still host Russia-based workers in the IT

[11] Stanislav Tkachenko, "The Political Economy of Russian Information & Communication Technologies," PONARS Eurasia Policy Memo No. 533, June 2018, https://www.ponarseurasia.org/wp-content/uploads/attachments/Pepm533_Tkachenko_June2018.pdf

sector, design sector, marketing, and related areas, and they lack strict processes to enable the association of individual workers with a particular location. Until there is a direct block on foreign firms operating inside Russia and hiring Russia-based workers, those companies will continue supporting a Russian tech sector with high wages that is sheltered from the consequences of Russia's war. This paper recommends minimally that Russia-based workers be subject to the same deemed export qualifications as would be required if that same worker were based in a sanctioning nation, especially if any companies in the ownership structure deal with items or knowledge of potential use to Russia's military operations.

Beyond physical infrastructure and software, technology-consulting and related company-based training infrastructure should be limited from servicing Russia-based workers. Additionally, Russian IT products and services should be import-controlled in sanctioning-nations' markets, to deprive the Russian government of additional revenues and avoid compromising sanctioning-nation digital systems.

Part IV. IT To Be Sanctioned

The following categories attempt to define the technologies and supporting intellectual property and infrastructure that should be sanctioned in order to achieve the desired objectives. The list is intended to be applied to all critical sectors of the economy.

- Software/Firmware (including network and web-enabled)
    - Cybersecurity/Protection
    - Operating Systems
    - Device Controllers/Interfaces
    - Network Management/Packet Processing and Monitoring
    - Messaging/Communication/VoIP
    - Logistics/Operations/Infrastructure Management
    - Financial/Payments (including fintech, cryptocurrencies, NFTs)
    - Databases/Storage/Blockchain
    - Data Processing/Analysis
    - Signal Processing
    - Cryptographic Services/Encryption
    - Statistical/Numerical Computing/Libraries
    - Scientific Computing and Infrastructure (including Physics/Geophysics/Space)
    - Environment/Energy/Modelling
    - Gaming
    - CAD/CAM/BIM
    - Computer Vision
    - Productivity/Creative
    - User Account and User Data Instances and Management
    - Web Applications and Related Software
    - Web Technology Frameworks
    - Website DNS and Network Traffic Management
    - Website Mail and Communication Services
    - Web Advertising and Programmatic Tracking
    - Social Media and Related Functionality
    - Identity Management and Authentication
    - Content Management Systems
    - Monitoring and Testing Infrastructure/Tools
    - Code Management/Testing/Deployment
    - Edge Infrastructure, Content Delivery Networks
- Cloud Computing/Cloud Services/Cloud Storage/Infrastructure Management
- Sensors, IoT Devices, Data Management Services, Remote Sensing
- Industrial Machinery/Robotics/Hydraulics/Heavy Machinery Controllers and their components
- Software Licence and Update Management
- Technology Maintenance/Support/Remote Service/Consulting
- Hardware or integrated components supporting any of the above capabilities or their creation
- Technology Outsourcing/Remote Employment

Conclusion

The International Working Group on Russian Sanctions aims to provide expertise and experience to governments and companies around the world by assisting with the formulation of sanctions proposals that will increase the cost to Russia of invading Ukraine and that will support democratic Ukraine in the defense of its territorial integrity and national sovereignty. The sliding scale approach of incrementally increasing pressure tends to enable Russian adaptation, not a reassessment of war aims. Putin intends to continue annexing Ukrainian territory and subjugating Ukraine under Russia's sphere of influence. As sanctioning nations gradually increase pressure, Putin will shift the resources he is using. Consequently, our goal must be to decrease the resources at his disposal.

The recommendations in this paper aim to degrade Russian military capabilities in the field over the short, medium, and long term. They attempt to degrade Russia's ability to maintain critical modern infrastructure to the point that it may also interfere with Russia's strategic military command and control infrastructure (lack of spare parts, incompatibilities, lack of knowledge from foreign entities, etc.). Recommendations outlined in this paper further aim to degrade Putin's information warfare resources, as an indirect means to reduce support within Russian society for his war. A third goal of our recommendations is to degrade the Russian economy more generally, in the hope that suffering Russian elites and society will eventually demand an end to Putin's war as a path to sanctions relief.

It is important now to act swiftly and decisively to prevent Russia from accessing and using ideas and technology from nations that oppose this war, deploying these assets to wreak havoc and destruction in Ukraine, and growing the future burden to be borne by sanctioning nations in rebuilding Ukraine and the global security infrastructure.

Appendix I. Technology Company Case Studies

We highlight below several examples of the most impactful foreign entities still providing hardware, software, firmware, and services in Russia.

Many of these companies have already taken steps to limit their activities on the Russian market and/or assist Ukraine. With the recommendations we outlined, these companies have the opportunity to take significant further actions to limit harm to the people of Ukraine and the costs borne by the populations of sanctioning nations who are paying for the damage taking place on Ukrainian soil.

As the war continues, it is necessary to evaluate the broad physical and economic (direct and indirect) damage associated with the continued availability of certain services within Russia and any potential ambiguity in the use of their technology. We trust that these companies – and the thousands of others still engaged in the technology ecosystem supporting Russia – will want to work in good faith with sanctioning-nation governments to find fast, effective, and complete solutions to limit further damage.

International Business Machines (IBM)

- **What:** IBM Operating systems; Red Hat; servers and hardware components/spare parts; middleware; components including microchips, switches, routers, and other communication devices; databases and databases as a service; cloud infrastructure; payments processing infrastructure; data processing and storage services; business intelligence services; B2B and government software; industry-specific logistics and financial services and similar software, consulting, or hardware provided through any subsidiary globally.
- We are concerned about the ongoing availability of IBM products and technology services within Russia, and the exploitation of these capabilities by existing clients throughout software stacks that enable military command and control, coordination of the military operation, supply, logistics, modelling, training, and similar activities.

Meta

- **What:** Facebook, Messenger, WhatsApp, Instagram, related services.
- Facebook and Instagram were both banned by the Russian government, showing that entities within sanctioning nations and their governments have little control over access to reliable information in Russia. WhatsApp was not banned, in part because so many Russian government officials and military officers use the platform, making it accessible for non-governmental civil society and opposition leaders as well. Facebook took several exemplary steps to block ads completely for Russian entities globally and ramped up efforts to weed out networks of fake accounts. Meta platforms also play a vital role in providing content and communications inside Ukraine. However, secure messaging networks such as WhatsApp do continue to support military coordination, and misinformation from Russian and linked accounts remains a large challenge. Although difficult (but not impossible), Meta should take greater measures to disable

WhatsApp's uses for supporting the war while sustaining its uses for non-governmental communications.

Twitter

- **What:** Twitter, Twitter Ads (outside Russia).
- Services used to spread disinformation outside Russia's borders, which in turn imposes coordination costs and difficulties within sanctioning nations, intensifies geopolitical tensions, and furthers the Kremlin's aims.

Apple

- **What:** Apple devices, Apple App Store, Apple communication protocols and services, Apple cybersecurity services and device protection services/libraries.
- Apple's devices and capabilities through the Apple App store continue to be used in military settings for communication, logistics, reconnaissance, remote control of military assets, and similar military and quasi military uses. Apple took strong and visible actions to prevent the replenishment of device inventory in the Russian market, although Apple devices continue to cross the border via so-called parallel import schemes. Apple Pay services were blocked due to financial sanctions against Russia.

Google (Alphabet)

- **What:** Google hardware devices; Android Operating Systems; Google Play; Google Cloud; Google Maps, Earth, and Location-based Services; Gmail and Secure Communication Services; Domain Administration/Hosting Services; Office/Productivity Software; Software Updates.
- Since the start of the war, Alphabet's Google has blocked ads in Russia, blocked global ads for any entity based in Russia, blocked thousands of suspicious accounts on YouTube, and supported the Ukrainian government in identifying and responding to cyber threats on key infrastructure. Google was the first company to be presented the Ukrainian Peace Prize for its willingness to support Ukraine technologically and philanthropically. YouTube remains an important source of real information about the war for Russians living in Russia, and it supports the main Russian independent media and opposition channels providing content inside Russia.
- At the same time, Google devices and devices running Android operating systems are used in battlefield communications in order to perform real-time reconnaissance, control equipment remotely, pass messages between units, and share information with logistics units where encrypted radio communications are less effective or where troops lack specifically issued equipment. Google Play supports configuration of devices to achieve these aims. Software updates continue to protect these devices, and location-based services serve as a secondary layer of situational awareness (e.g., Google Earth) for troops. Google Docs and related services provide basic knowledge-sharing and collaborative capabilities within Russia for the organisation of military recruiting, training, and regional military planning activities. Google Cloud infrastructure

and services continue to operate for a variety of Russia-based entities who may be supporting Russia's military operations and planning.

Microsoft

- **What:** Windows, Exchange, Office/Outlook/Teams, Microsoft Bing/Ads, Skype, Azure Cloud, Networking protocols and services, GitHub (repositories managed from Russia, by Russian entities, or connected to Russian infrastructure for deployment/testing), Microsoft hardware devices (e.g., Surface), internet information services, software updates, maintenance and customer support.
- Microsoft halted new sales of all products in Russia and has worked hard to help the Ukrainian government and many other Ukrainian organisations to protect themselves from Russian cyber-attacks. However, Microsoft's core services, from Exchange to Office and Azure cloud infrastructure continue to be available to the vast majority of Microsoft's pre-war Russian client base. We are concerned about the exploitation of this infrastructure for military-adjacent and direct military uses, communication and logistics, reconnaissance, and a variety of quasi military use cases that are destructive to Ukraine, and where ties to Russia's government may be difficult to ascertain. We are further worried that many operational and logistical activities are taking place across Russia in support of the military and training through Microsoft capabilities like Office365 and similar services. Not all such capabilities can feasibly be removed, but where capabilities can be restricted, there is an opportunity to leave large gaps in operational capacity, requiring large resource commitments for Russia to adapt.

Cloudflare

- The Ukrainian government asked Cloudflare to cease all operations in Russia at the start of the war. Cloudflare refused and stated that this would lead to a curtailment of information freedom within Russia, but this is a defective argument. Russia's government controls internet freedom in Russia, and any Cloudflare-protected website that the government would like to control would quite easily be subject to measures that would ensure control. In the meantime, Cloudflare software makes Russian government, military, and misinformation infrastructure more resilient and better able to operate and damage sanctioning-nation interests.

Note: The inclusion of affiliations is for identification purposes only and does not represent an endorsement of shared views with the co-signer.

Yaroslav Azhniuk, Entrepreneur and Co-Founder, Petcube.

Tania Babina, Assistant Professor of Finance, Columbia Business School, Columbia University; Co-organizer of the Economists for Ukraine group.

Dr. Andriy Boytsun, Founder and Editor of the Ukrainian SOE Weekly; Independent Corporate Governance Consultant; Former Member of the Strategic Advisory Group for Supporting Ukrainian Reforms.

Anne L. Clunan, Associate Professor of National Security Affairs, Naval Postgraduate School, and Faculty Affiliate, Center for International Security and Cooperation (CISAC), Stanford University. *The views here are my own, and not those of the U.S. Navy, Department of Defense, or Government.*

Tatyana Deryugina, Associate Professor, Department of Finance, University of Illinois - Urbana-Champaign; Co-organizer of the Economists for Ukraine group.

Anastassia Fedyk, Assistant Professor of Finance, the Haas School of Business, University of California - Berkeley; Co-organizer of the Economists for Ukraine group.

Yuriy Gorodnichenko, Quantedge Presidential Professor of Economics, Department of Economics, University of California - Berkeley; Co-organizer of the Economists for Ukraine group.

Denis Gutenko, Ukrainian Emerging Leaders Program Fellow, Stanford University, and Former Head of the State Fiscal Service of Ukraine.

James Hodson, Director and Chief Executive Officer, AI for Good Foundation; Co-organizer of the Economists for Ukraine group.

Eric Johnson, Former Managing Director, Cambridge Associates, and Former National Security Council Staff, White House Situation Room.

Bronte Kass, Program Manager, Freeman Spogli Institute for International Studies (FSI), Stanford University; Assistant Coordinator, International Working Group on Russian Sanctions.

Craig Kennedy, Center Associate, Davis Center for Russian and Eurasian Studies, Harvard University.

Michael McFaul, Director, Freeman Spogli Institute for International Studies (FSI), Professor of Political Science, and Hoover Institution Senior Fellow, Stanford University; Coordinator, International Working Group on Russian Sanctions.

Benjamin Moll, Professor, London School of Economics and Political Science.

Jacob Nell, Senior Research Fellow, Kyiv School of Economics, and Former Chief Russia Economist, Morgan Stanley.

Olesksandr Novikov, Head of the National Agency on Corruption Prevention, Ukraine.

Lukasz Rachel, Assistant Professor of Economics, University College London.

Dr. Benjamin L. Schmitt, Project Development Scientist, Harvard University; Senior Fellow for Democratic Resilience, Center for European Policy Analysis; Rethinking Diplomacy Fellow, Duke University Center for International and Global Studies.

Andrey Simonov, Associate Professor, Columbia Business School, Columbia University.

Daria Sofina, National Agency on Corruption Prevention, Ukraine.

Ilona Sologub, Scientific Editor, Vox Ukraine; Co-organizer of the Economists for Ukraine group.

Jeffrey Sonnenfeld, Senior Associate Dean and Professor, Yale School of Management.

Kyrylo Sygyda, Co-Founder, Reface, Zibra, Pawa.

Pavlo Verkhniatskyi, Managing Partner, Director, COSA.

Yuriy Vitrenko, CEO, Naftogaz of Ukraine.