



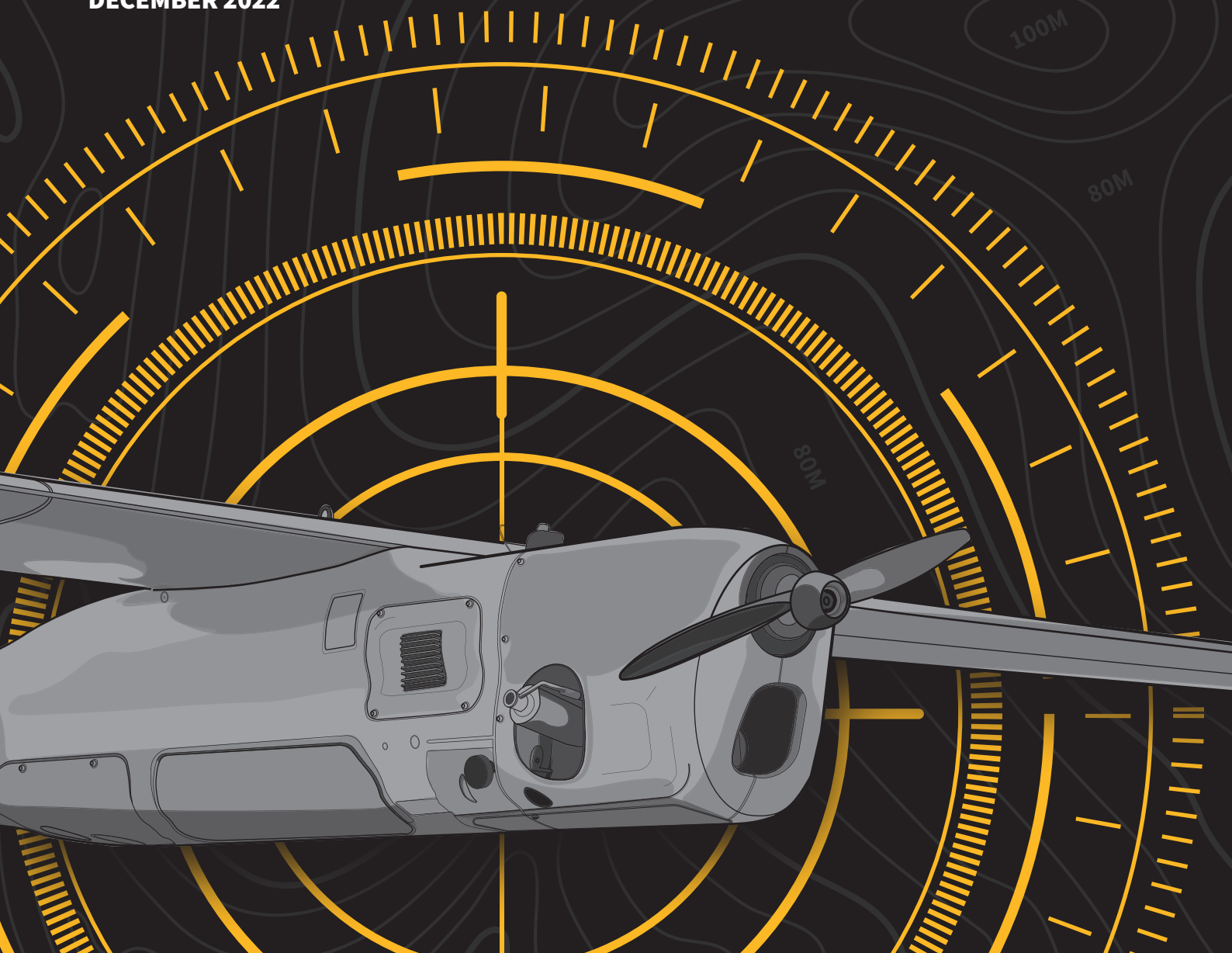
# THE ORLAN COMPLEX

## TRACKING THE SUPPLY CHAINS OF RUSSIA'S MOST SUCCESSFUL UAV



JAMES BYRNE, JACK WATLING, JUSTIN BRONK, GARY  
SOMERVILLE, JOE BYRNE, JACK CRAWFORD AND JANE BAKER

DECEMBER 2022



# The Orlan Complex

## DISCLAIMER

This document has been prepared by RUSI for informational purposes only (the 'Permitted Purpose'). While all reasonable care has been taken by RUSI to ensure the accuracy of material in this report (the 'Information'), it has been obtained primarily from fieldwork in Ukraine and open sources and RUSI makes no representations or warranties of any kind with respect to the Information.

You should not use, reproduce or rely on the Information for any purpose other than the Permitted Purpose. Any reliance you place on the Information is strictly at your own risk. If you intend to use the Information for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps or otherwise deal with any named person or entity), you must first undertake and rely on your own independent research to verify the Information.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of any of the Information by you or any third party. References to RUSI include its directors and employees.

For this report, the authors have processed company, entity and individual names recorded in Russian and Chinese. In some instances, names of companies, entities and individuals have had to be translated or transliterated. Every effort has been made to ensure accuracy in translation/transliteration, and the authors do not accept liability for any unintentional errors made in this regard.

## METHODOLOGY

For this report, RUSI's Open-Source Intelligence and Analysis (OSIA) and Military Sciences departments used extensive datasets of components and microelectronics sourced from disassembled Russian weapons either captured or expended in Ukraine since February 2022. These compilations of technical assessments were databased, standardised and categorised to enable further analysis.

Physical inspection of the platforms contained in this report by RUSI during fieldwork confirmed the authenticity and accuracy of this data, which was also compared to product descriptions and serial numbers published by a wide variety of manufacturers. It should be noted that grey and black markets for counterfeit components and microelectronics are a global problem, meaning that fool-proof corroboration is a challenging endeavour. Given the evidence assessed here and the long history of Soviet and Russian military procurement efforts targeting the world's leading technology and microelectronic companies, the research team operated under the assumption that the majority of these parts were likely genuine. Assessments conducted internally by the Russian government, and seen by the authors, highlighting critical dependence on a number of foreign manufacturers, increases the confidence that the components identified in Russian weapons are genuine.

This data was then married with a range of other sources, such as shipment-level trade data, import and export declarations, court records, financial information sourced by Reuters and iStories, and corporate records in Russian in an attempt to better understand a particular Russian procurement network while also placing the Orlan-10, a Russian UAV, in its tactical and operational context.

### IDENTIFICATION OF INDIVIDUALS, COMPANIES AND GOVERNMENTS IN THIS REPORT

The purpose of this report is to understand and explain how the Russian military depends on Western technology. To achieve this purpose, it identifies a number of individuals/companies/governments who are believed to be involved in the designing and manufacturing of components which have been acquired by the Russian military and are used in their military hardware. For the avoidance of doubt, RUSI does not impute any allegations of wrongdoing on the part of these individuals/companies/governments and makes no representations or assertion that these individuals/companies/governments have any involvement in any sanctions evasion-related activity or are involved in directly or indirectly supplying the Russian military and/or Russian military customers in breach of any international (or their own domestic) laws or regulations restricting or prohibiting such action, unless expressly stated in the report.

### ACKNOWLEDGEMENTS

RUSI would like to thank several people and partners who have helped with this report,

including Dr Daniel Salisbury, Dr Aaron Arnold and Thomas Ewing. RUSI would also like to thank the Economic Security Council of Ukraine and Altana Technologies, whose ‘Altana Atlas’ data platform helped us track semiconductor and microelectronic goods as they moved through the international trading system.

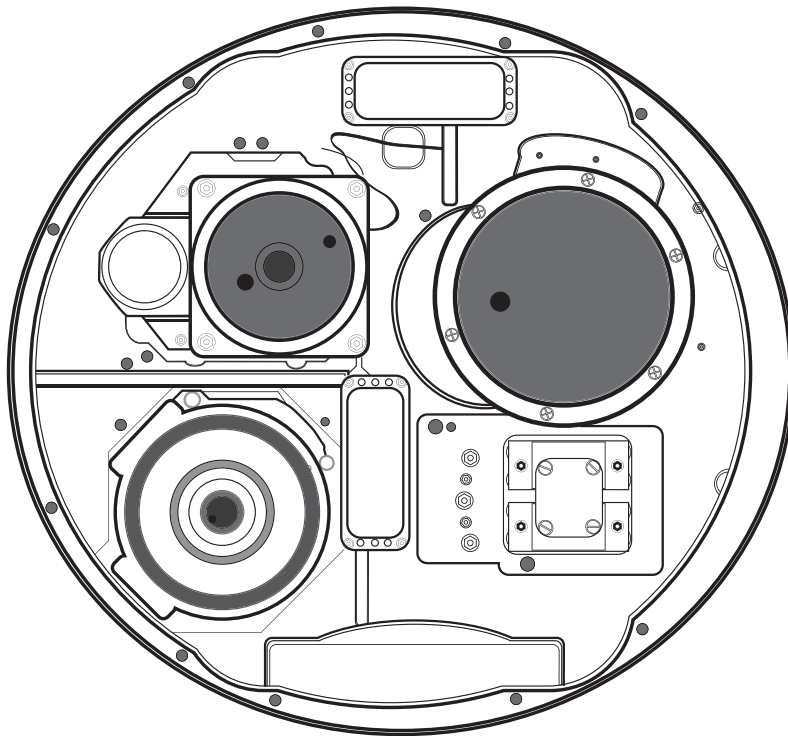


### COPYRIGHT

© Royal United Services Institute for Defence and Security Studies, 2022



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <<http://creativecommons.org/licenses/by-ncnd/4.0/>>.



The outline of the Orlan-10 EO sensor. Source: RUSI

# Contents

EXECUTIVE SUMMARY	5
INTRODUCTION	7
SECTION 01: BUILT IN RUSSIA, MADE ABROAD	9
Built in Russia, Made Abroad	9
The Special Technology Centre	10
SECTION 02: THE MEN BEHIND THE CURTAIN	12
The Men Behind the Curtain	12
Fuzzy Logic: STC's Links to SMT-iLogic	13





**SECTION 03: ILLICIT PROCUREMENT** 16

Illicit Procurement 16

Chinese Suppliers 19

Anton Trofimov 20

**CONCLUSION** 22

# Executive Summary

A joint investigation between RUSI, Reuters and iStories has found that Russian companies closely associated with the St Petersburg-based Special Technology Centre Limited Liability Company (STC LLC or STC) – the Russian military-affiliated manufacturer of the Orlan-10 UAV<sup>1</sup> – have drastically increased imports of critical Western-manufactured components since the February 2022 invasion of Ukraine began.

These imports will likely enable the Armed Forces of the Russian Federation (AFRF) to maintain and expand production of the country's most successful UAV – a platform that sits at the heart of the country's warfighting capabilities and enables the AFRF to rain accurate fire down on Ukrainian formations.<sup>2</sup>

Financial records, customs data, court records, Russian company filings and a range of other open sources indicate that many of these Western-manufactured imports are likely being procured by a St Petersburg-based company named SMT-iLogic<sup>3</sup> on behalf of STC,<sup>4</sup> which was first sanctioned by the US government in December 2016 for supporting Russia's interference in the 2016 US Presidential election.<sup>5</sup>

These components, which are critical both to

Russia's plans to expand UAV production and its ongoing operations in Ukraine, are being shipped to Russia by a variety of distributors based in the United States, Europe, China, South Korea and Hong Kong.<sup>6</sup>

In many cases, these exporters appear to be operated by Russian nationals or expatriates based abroad with limited public profiles. In one such case, a US company owned by an individual with Russian and American citizenship named Igor Kazhdan shipped large volumes of export-controlled components to SMT-iLogic and another company named Device Consulting, also based in St Petersburg, in violation of US export controls.<sup>7</sup>

Some of SMT-iLogic's largest suppliers since the start of Russia's invasion have been a range of Hong Kong companies,<sup>8</sup> some with a history of evading sanctions and providing military equipment to the Chinese government.<sup>9</sup>

Networks such as those profiled in this report are core to Russia's ability to procure advanced microelectronics for its weapons programs. As the United States and its allies seek to restrict Russia's ability to access the world's most advanced technologies, trade restrictions such as export

- 1 Специальный технологический центр [Special Technology Centre], 'Вооружение и военная техника' ['Weapons and military technology'] <<https://www.stc-spb.ru/activities/vooruzhenie-i-voennaya-tekhnika/>>, accessed 6 December 2022; Über Zalizyaken Ukroppen, "'Orlan' Drones – The Sea Eagles of St. Petersburg', <<https://informnapalm.org/en/orlan-drones-the-sea-eagles-of-st-petersburg/>>, accessed 7 November 2022; Avia-Pro, 'Orlan-50. Specifications. A photo.', <<https://avia-pro.net/blog/orlan-50-tehnicheskie-harakteristiki-foto/>>, accessed 7 November 2022.
- 2 Author fieldwork in Ukraine.
- 3 'SMT-iLogic' is the registered name of the company. The authors were unable to ascertain if 'SMT' is an acronym for anything.
- 4 Stephen Grey, Maurice Tammam and Maria Zholobova, 'The global supply chain feeding Russia's killer drones', Reuters, 15 December 2022.
- 5 White House Office of the Press Secretary, 'FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment', 29 December 2016, <<https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and>>, accessed 11 November 2022; International Trade Compliance Blog, 'US Sanctions Russian Intelligence and Security Services in Response to Alleged Election-Related Hacking', 30 December 2016, <<https://www.internationaltradecomplianceupdate.com/2016/12/30/us-sanctions-russian-intelligence-and-security-services-in-response-to-alleged-election-related-hacking/>>, accessed 11 November 2022.
- 6 Trade data supplied by third-party commercial provider.
- 7 United States of America v. Igor Kazhdan, also known as 'Alex Stanton', 'Criminal Complaint', United States District Court for the Southern District of Florida, 0:22-mj-06066-PMH, 29 March 2022, see Pacer.gov, <<https://pacer.login.uscourts.gov/>>.
- 8 Trade data supplied by third-party commercial provider.
- 9 James Byrne, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds and Jane Baker, 'Silicon Lifeline: Western Microelectronics at the Heart of Russia's War Machine', RUSI Special Report, 8 August 2022.

controls and sanctions are emerging as core tools available to policymakers.

This report highlights methodologies that can be used by state and non-state actors alike in combating Russian sanctions evasion networks. Approaches demonstrated in this report, including the use of open-source information, integration of modern data analysis methods, and the use of commercial technologies, can successfully identify sanctions evasion networks in detail and at scale. If governments wish to slow shipments to critical Russian military programmes such as the Orlan-10, they should:

- Increase their ability to amass, analyse, and action open-source information through investments in data storage, processing, and visualization. Artificial intelligence will be a core part of several capabilities that can materially improve export control and sanctions enforcement, such as the creation of graph databases showing historical trading relationships, entity resolution, text extraction, machine translation, and geolocation.
- Increase use of commercial analytics and data providers. As demonstrated in this report, commercial tools available today can allow for the identification of export control and sanctions evasion networks at scale.
- Curate the data environment to ensure that actionable information flows to enforcement authorities to the maximum degree allowed by law. Enforcement authorities should work with Congress to pass laws that expand visibility into trade, corporate and risk data that would provide actionable intelligence on sanctions evasion networks, while safeguarding privacy and civil liberties.
- Adopt systems that allow for data-driven interoperability with allies, including by adopting information architectures that allow for easy and secure sharing of information. The US is just one node in a global trading web used by sanctions and export control evaders – successful

enforcement necessarily depends on joint action. The US can bring to bear open-source information and federated data architectures to share information with partners, even where sharing classified information is undesirable.

- Partner with, and make greater use of, non-state analytical organisations with expertise in identifying illicit activity using open-source information. As this report demonstrates, non-state analytical actors possess significant expertise in identifying sanctions and export control evasion. The US and its allies should engage robustly with these organisations to share leads, investigative techniques, tools and data.

Fundamentally, improving this capability this will entail investments in the government's ability to amass, analyse, and action large quantities of publicly-available and commercial information. This will allow the government to more quickly and comprehensively identify and address gaps in its enforcement of sanctions and export controls, allowing it to:

- Rapidly sanction entities and individuals involved in the illicit supply chain of components to the AFRF.
- Identify and prosecute individuals knowingly evading sanctions and export controls to ship components to the AFRF or those acting on their behalf.
- Strengthen the monitoring of components and microelectronics moving to Russia and the identity of end-users to which they are being shipped.
- Improve guidance and expand capacity-building operations for private sector companies and financial institutions engaged in exporting or financing these component flows.

# Introduction

The Orlan-10 UAV has proven to be one of the most critical components of the Armed Forces of the Russian Federation's (AFRF) lethality in Ukraine. Designed and manufactured by Russia's Special Technology Centre Limited Liability Company (STC LLC or STC),<sup>10</sup> the Orlan-10 is a sophisticated yet relatively affordable UAV, costing approximately \$87,000–120,000 per system.<sup>11</sup> The UAV can carry a wide range of military payloads, enabling it to conduct a variety of missions and to be used in combination with other systems, including other UAVs, for more advanced combinations of effects.<sup>12</sup>

The most common and deadliest use of Orlan-10s by the AFRF in Ukraine is as part of an intelligence, surveillance and reconnaissance complex. The UAVs are used to locate Ukrainian troops and vehicles from medium altitudes and relay their positions for rapid artillery, missile and loitering munition strikes. When an Orlan-10 is overhead, Russian

artillery response times can be as short as three minutes from target detection, leaving those targets almost no time to escape the fire zone.<sup>13</sup> By contrast, response times when UAVs are not overhead are generally around 20 minutes, affording Ukrainian units the opportunity to relocate and avoid destruction.<sup>14</sup> The centrality of artillery firepower to battlefield tactics on both sides means that the presence or absence of Russian UAVs in Ukraine is a core determinant of Russian lethality.

The Orlan-10 is particularly challenging for Ukrainian ground forces to counter. It can reportedly reach speeds of at least 150km/h and a maximum altitude of 5,000 metres.<sup>15</sup> The ability to fly at these relatively fast speeds and high altitudes allows the Orlan-10 to operate beyond the range of most man-portable air-defence systems (MANPADS),<sup>16</sup> and also makes the UAV harder to detect and engage.<sup>17</sup>

10 Общество С Ограниченной Ответственностью 'Специальный Технологический Центр' (СТЦ) [Limited Liability Company 'Special Technology Centre']; INN: 7802170553. Also known as 'Special Technological Centre LLC'.

11 Worldwide Equipment Guide, 'Orlan-10', <[https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10\\_Russian\\_Unmanned\\_Aerial\\_Vehicle\\_\(UAV\)](https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10_Russian_Unmanned_Aerial_Vehicle_(UAV))>, accessed 11 November 2022.

12 These payloads include electro-optical, infra-red and thermal cameras; laser imaging, detection and ranging (LIDAR) sensors; and signals intelligence (SIGINT), electronic intelligence (ELINT), electronic warfare (EW) and data-relay capabilities.

13 Author fieldwork in Ukraine.

14 *Ibid.*

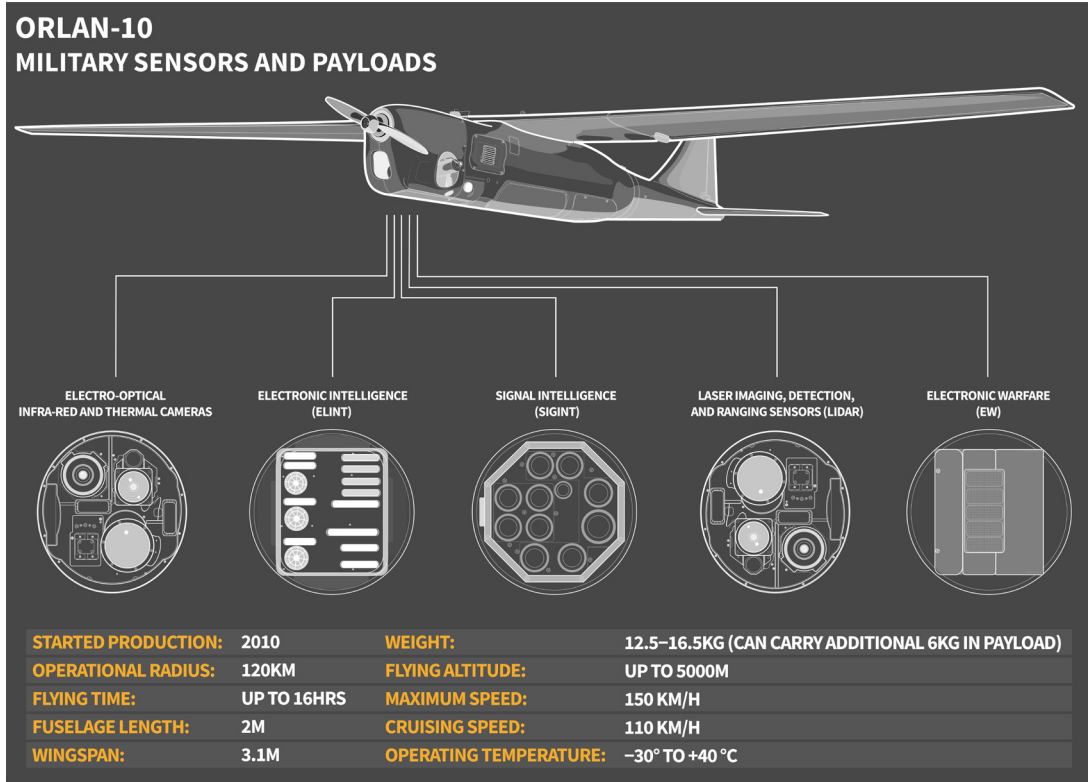
15 Worldwide Equipment Guide, 'Orlan-10', <[https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10\\_Russian\\_Unmanned\\_Aerial\\_Vehicle\\_\(UAV\)](https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10_Russian_Unmanned_Aerial_Vehicle_(UAV))>, accessed 11 November 2022.

16 For example, the US FIM-92 Stinger MANPADS has a range maximum of approximately 4,000 metres. Worldwide Equipment Guide, 'FIM-92 Stinger American Man-Portable Air-Defense System (MANPADS)', <[https://odin.tradoc.army.mil/WEG/Asset/FIM-92\\_Stinger\\_American\\_Man-Portable\\_Air-Defense\\_System\\_\(MANPADS\)](https://odin.tradoc.army.mil/WEG/Asset/FIM-92_Stinger_American_Man-Portable_Air-Defense_System_(MANPADS))>, accessed 9 November 2022.

17 Author fieldwork in Ukraine.



Figure 1: Orlan-10 Military Sensors and Payloads



Source: OE Data Integration Network - US Government; Information provided to RUSI; graphic designed by RUSI OSIA.

Additionally, the Orlan-10 boasts hardened radio datalinks with frequency-hopping capabilities and an accurate inertial navigation system that renders it difficult to effectively jam using electronic warfare (EW).<sup>18</sup>

In addition to artillery spotting, the AFRF uses the Orlan-10 for effective suppression and destruction of enemy air defence (SEAD/DEAD) operations in Ukraine. For such missions, a high-flying Orlan-10 with an EW payload baits Ukrainian SA-8 and SA-11 surface-to-air missile (SAM) systems, with

its survivability boosted by its capacity to jam SA-8 missile proximity fuses.<sup>19</sup> Once a SAM is launched to engage the UAV, a second Orlan-10 at a lower altitude geolocates the SAM’s launch system using electronic intelligence capabilities and cues a third Orlan-10 which uses an electro-optical payload to designate the launch system as a target for rapid artillery or missile strikes from Russian forces.<sup>20</sup> Given this flexibility and effectiveness from a mass-produced system, constraining and countering Orlan-10s is one of the Ukrainian military’s top priorities.

18 *Ibid.*

19 Justin Bronk, Nick Reynolds and Jack Watling, ‘The Russian Air War and Ukrainian Requirements for Air Defence’, RUSI Special Report, 7 November 2022.

20 *Ibid.*

# Built In Russia, Made Abroad

Behind the impressive success of Russia's most prevalent UAV system is the St Petersburg-headquartered STC, a limited liability company with extensive connections to the country's leading research centres and Russia's expansive military industrial complex. However, while the Orlan-10 is designed and built in Russia by a range of scientists and engineers from flagship Russian military research institutes, its construction is highly dependent on Western technology and components historically procured through suppliers based in the US, Europe and East Asia.

Fieldwork conducted by RUSI in Ukraine over the course of 2022 confirmed that the sub-systems of the Orlan-10 are heavily reliant on foreign-made microelectronics. This is particularly the case for a range of products such as the microcontrollers, global navigation satellite system (GNSS) receivers and pressure sensors that enable the UAV to collect and transmit relevant data to the operator, sometimes over 100 km away.<sup>21</sup>

Some of these Western-manufactured components are also subject to export controls, meaning that

those seeking to ship them abroad require a licence to do so. Even before Russia's February 2022 full-scale invasion of Ukraine, US manufacturers could not legally export goods subject to US Department of Commerce Export Administration Regulations (EAR)<sup>22</sup> to Russian defence companies—and certainly not to designated entities.

For many of Russia's designated military entities, this has led to a need for illicit procurement tactics, including the use of front companies and transshipment hubs to move goods through the international trading system.<sup>23</sup>

Financial records for STC, acquired by Reuters and iStories, indicate that the company has remitted large volumes of money to a range of Russian companies involved in the electronics and radiocommunication businesses.<sup>24</sup> One of the largest recipients is an entity named SMT-iLogic, a company based in St Petersburg that not only imports large volumes of microelectronics and components used in the Orlan-10 to Russia but also has additional extensive connections to STC.<sup>25</sup>

21 Worldwide Equipment Guide, 'Orlan-10', <[https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10\\_Russian\\_Unmanned\\_Aerial\\_Vehicle\\_\(UAV\)](https://odin.tradoc.army.mil/mediawiki/index.php/Orlan-10_Russian_Unmanned_Aerial_Vehicle_(UAV))>, accessed 11 November 2022.

22 This includes any goods classified as ECCN or EAR99; US Department of Commerce, Bureau of Industry and Security, 'Entity List', <<https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>>, accessed 16 November 2022. For more on the application of export controls to shipments of goods to Russian companies, particularly in the context of Russia's invasion of Ukraine, see James Byrne et al., 'Silicon Lifeline', pp.15-17.

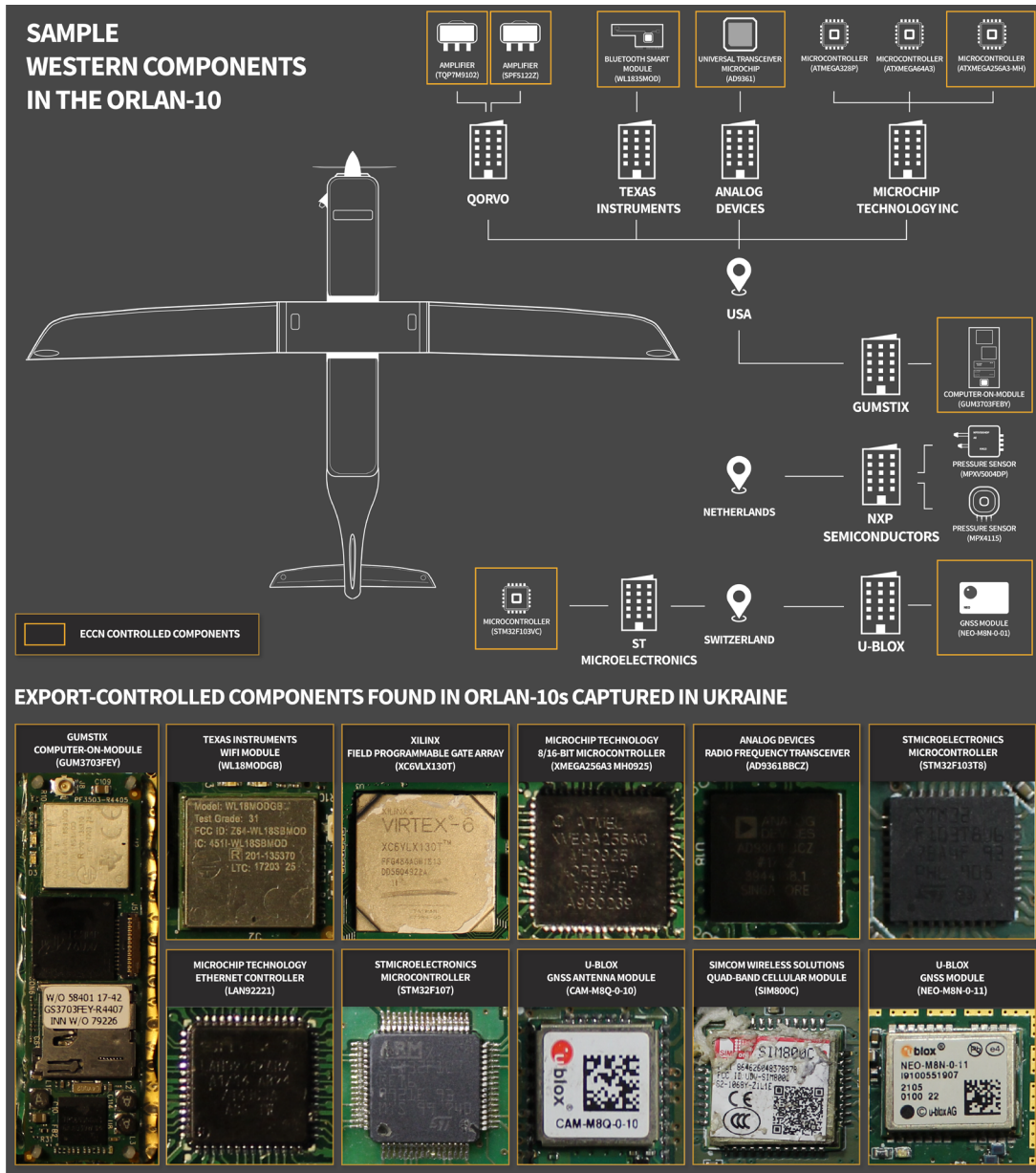
23 Byrne et al., 'Silicon Lifeline'.

24 Stephen Grey, Maurice Tammam and Maria Zholobova, 'The global supply chain feeding Russia's killer drones', Reuters, 15 December 2022.

25 *Ibid.*



Figure 2: Foreign Components in the Orlan-10 UAV



Source: OE Data Integration Network – US Government; Centre for Defence Reform Ukraine; RUSI fieldwork in Ukraine graphic designed by RUSI OSIA.

**THE SPECIAL TECHNOLOGY CENTRE**

Founded over twenty years ago, STC designs and manufactures radio and communications equipment for a range of customers, including military systems<sup>26</sup>

and the Orlan-10.<sup>27</sup> In addition to the Orlan-10, STC manufactures other UAVs including the Orlan-1, the Orlan-2, the Orlan-30 and the Orlan-50.<sup>28</sup>

26 Специальный технологический центр, [Special Technology Centre], ‘Вооружение и военная техника’ [‘Weapons and military technology’] <<https://www.stc-spb.ru/activities/vooruzhenie-i-voennaya-tehnika/>>, accessed 6 December 2022.  
 27 Специальный технологический центр, [Special Technology Centre], ‘Наша продукция’ [‘Our products’] <<https://www.stc-spb.ru/production/>>, accessed 6 December 2022.  
 28 Über Zalizyaken Ukropfen, “Orlan” Drones – The Sea Eagles of St. Petersburg’, <<https://informnapalm.org/en/orlan-drones-the-sea-eagles-of-st-petersburg/>>, accessed 7 November 2022; Avia-Pro, ‘Orlan-50. Specifications. A photo.’, <<https://avia-pro.net/blog/orlan-50-tehnicheskie-harakteristiki-foto/>>, accessed 7 November 2022.

## The Orlan Complex

STC also appears to be engaged in a range of clandestine activities separate from the design and manufacture of military UAVs. In December 2016, for example, the US Department of the Treasury sanctioned STC alongside Russia's Federal Security Service (FSB) and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU) for conducting malicious cyber-related activities.<sup>29</sup> According to the US Department of the Treasury, STC was designated because it had supported the GU's interference campaign targeting the 2016 US Presidential election.<sup>30</sup> Three years later, the cyber security company

Lookout alleged that STC was developing advanced mobile spyware designed to infect devices using Google Android.<sup>31</sup> The spyware, dubbed Monokle, reportedly targeted a small number of individuals, including those researching Russian-backed militias in Syria.<sup>32</sup>

Following Russia's 2022 invasion of Ukraine, STC was further designated by the US,<sup>33</sup> the UK,<sup>34</sup> Canada,<sup>35</sup> Taiwan<sup>36</sup> and Japan.<sup>37</sup> These designations identified STC's role in aiding Russia's invasion and aimed to further restrict the company's imports of foreign technology.

---

29 US Department of the Treasury, 'Issuance of Amended Executive Order 13694; Cyber-Related Sanctions Designations', press release, 29 December 2016, <<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20161229>>, accessed 7 November 2022.

30 White House Office of the Press Secretary, 'FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment', 29 December 2016, <<https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and>>, accessed 11 November 2022; International Trade Compliance Blog, 'US Sanctions Russian Intelligence and Security Services in Response to Alleged Election-Related Hacking', 30 December 2016, <<https://www.internationaltradeupdate.com/2016/12/30/us-sanctions-russian-intelligence-and-security-services-in-response-to-alleged-election-related-hacking/>>, accessed 11 November 2022.

31 Apurva Kumar, 'Lookout Discovers New Mobile Surveillanceware Developed by Russian Defense Contractor Special Technology Center', Lookout, 24 July 2019, <<https://www.lookout.com/blog/monokle>>, accessed 11 November 2022.

32 Reuters, 'Russian Defense Contractor Developing Smartphone Spyware, U.S. Firm Says', *Moscow Times*, 24 July 2019, <<https://www.reuters.com/article/us-cyber-russia-smartphones-idUSKCN1UJ1OZ>>, accessed 11 November 2022.

33 This effectively denies them the ability to import goods including the microelectronics necessary to build their systems from the US-designated EAR99; US Department of Commerce, Bureau of Industry and Security, 'Additions of Entities to the Entity List', 87 FR 34154 (part 744), <<https://www.federalregister.gov/documents/2022/06/06/2022-12144/additions-of-entities-to-the-entity-list>>, accessed 11 November 2022; US Department of Commerce, Bureau of Industry and Security, 'Supplement No. 4 to Part 744 - ENTITY LIST', <<https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file>>, accessed 11 November 2022.

34 UK Foreign, Commonwealth & Development Office, 'The UK Sanctions List', <<https://www.gov.uk/government/publications/the-uk-sanctions-list#:~:text=The%20UK%20government%20publishes%20the,of%20reasons%20for%20the%20designation>>, accessed 15 November 2022.

35 Government of Canada, 'Consolidated Canadian Autonomous Sanctions List', <[https://www.international.gc.ca/world-monde/international\\_relations-reactions\\_internationales/sanctions/consolidated-consolide.aspx?lang=eng](https://www.international.gc.ca/world-monde/international_relations-reactions_internationales/sanctions/consolidated-consolide.aspx?lang=eng)>, accessed 15 November 2022.

36 Taiwan Ministry of Economic Affairs, Bureau of Foreign Trade, 'SHTC Entity List', 27 April 2022, <<https://icp.trade.gov.tw/ICP/Download.action?file=gxNvvh0VEIQV2cmwpPZfg%3D%3D>>, accessed 23 November 2022.

37 経済産業省 [Ministry of Economy, Trade and Industry], 'ウクライナ情勢に関する外国為替及び外国貿易法に基づく措置について' ['Regarding measures based on the Foreign Exchange and Foreign Trade Law regarding the situation in Ukraine'], 5 July 2022, <[https://www.meti.go.jp/policy/external\\_economy/trade\\_control/index.html](https://www.meti.go.jp/policy/external_economy/trade_control/index.html)>, accessed 23 November 2022.

# The Men Behind The Curtain

A closer look at the affiliations and activities of some of STC's executives reveals that the company is closely linked to the Russian military, as well as SMT-iLogic.

The leadership of STC is largely composed of highly accomplished Russian military scientists, at least two of whom are also employed by the SM Budyonny Military Academy of the Signal Corps,<sup>38</sup> a military university in St Petersburg for Russia's signal troops. These individuals are Aleksei Vasilievich Terentiev<sup>39</sup> and Oleg Vladimirovich Tsarik,<sup>40</sup> both recognised as 'Honoured Inventors of the Russian Federation'<sup>41</sup> – an accolade bestowed by the Russian president for an outstanding track record of inventions of national significance and major contributions to technological progress. The Academy's website notes that Terentiev has been serving at the SM Budyonny Academy since 1981, including as senior researcher and head

of the research laboratory.<sup>42</sup> Tsarik has also held a number of positions at the Academy since 1998, including as senior lecturer in the radio intelligence and electronic warfare department.<sup>43</sup> Terentiev has also been listed in the honour roll of best inventors at the Budyonny Academy,<sup>44</sup> while Tsarik was named best inventor of the year by the Russian Ministry of Defence in 2008.<sup>45</sup>

As of June 2022, Terentiev and Tsarik are two of seven shareholders in STC and some of the company's most prolific scientists.<sup>46</sup> Since 11 May 2010, STC has filed over 70 patents for radio-electronics and other communication technologies,<sup>47</sup> with the majority focused on military applications. Terentiev and Tsarik are listed as inventors on dozens of these patents, including several explicitly referencing technology related to the Orlan-10.<sup>48</sup>

38 Original Russian text: Военная академия связи имени Маршала Советского Союза С.М. Буденного.

39 Original Russian text: Алексей Васильевич Терентьев; INN: 781423758615.

40 Original Russian text: Олег Владимирович Царик; INN: 780432838287; Эксчек Про [Excheck Pro], 'ООО 'СТЦ' Учредители' ['LLC 'STC' Founders'], <<https://excheck.pro/company/7802170553/founders>>, accessed 11 November 2022.

41 Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], 'Заслуженные изобретатели Российской Федерации' ['Honoured Inventors of the Russian Federation'], <<https://vas.mil.ru/Nauka/Zasluzhennye-izobretateli-RF>>, accessed 14 November 2022.

42 Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], 'Терентьев Алексей Васильевич' ['Terentiev Alexei Vasilievich'], <<https://vas.mil.ru/Nauka/Zasluzhennye-izobretateli-RF/item/233710/>>, accessed 7 November 2022.

43 Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], 'Царик Олег Владимирович' ['Tsarik Oleg Vladimirovich'], <<https://vas.mil.ru/Nauka/Zasluzhennye-izobretateli-RF/item/233739/>>, accessed 15 November 2022.

44 Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], 'Терентьев Алексей Васильевич' ['Terentiev Alexei Vasilievich'], <<https://vas.mil.ru/Nauka/Zasluzhennye-izobretateli-RF/item/233710/>>, accessed 7 November 2022.

45 Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], 'Царик Олег Владимирович' ['Tsarik Oleg Vladimirovich'], <<https://vas.mil.ru/Nauka/Zasluzhennye-izobretateli-RF/item/233739/>>, accessed 15 November 2022.

46 Each of the seven shareholders holds an equally-distributed 14-15% of STC's shares; Russian Federal Tax Register, document dated 16 June 2022 from Sayari Analytics, <<https://sayari.com/>>, accessed 24 November 2022.

47 A Google Patents search on 14 November 2022 for patents filed by STC yielded 79 results, with some duplicates.

48 This includes RU2510044C1, RU2543078C1, RU2495527C1, and RU2775299C1, which was granted in June 2022.

Figure 3: Terentiev’s and Tsarik’s Biographies from the SM Budyonny Military Academy of the Signal Corps



Source: Russian Ministry of Defence; graphic and annotations by RUSI OSIA.

**FUZZY LOGIC: STC’S LINKS TO SMT-ILOGIC**

Despite producing large volumes of Orlan-10s and other UAVs that are highly dependent on foreign components and technology, STC does not appear to directly import any foreign components. However, Russian bank records for STC show the company paying tens of millions of dollars to SMT-iLogic.<sup>49</sup> Company records filed in 2017 show that both Terentiev and Tsarik had founded the company alongside other members of STC and were listed as shareholders at the time.<sup>50</sup>

SMT-iLogic’s website notes that the company was founded in November 2015 – a year after Russia’s initial incursion into Ukraine – by a group of ‘highly-qualified specialists in information and telecommunication technology.’<sup>51</sup> This statement is consistent with the list of individuals on the company’s filings with the Russian Federal Tax Registry over the years, which include Tsarik and Terentiev and several other scientists who also share patents with both inventors.<sup>52</sup> However, in August 2017, Tsarik, Terentiev and several other STC shareholders were removed from official

records of SMT-iLogic,<sup>53</sup> thus eliminating obvious evidence of SMT-iLogic’s links to STC.

Despite this, connections between STC and SMT-iLogic persist. For example, one of the current shareholders of SMT-iLogic is a Russian national named Aleksandr Mikhailovich Shepilov. Shepilov has been listed on SMT-iLogic’s corporate documents since November 2015, suggesting that he may have been one of the founders of the company.

Like his former colleagues, Shepilov is a prolific inventor and is named on at least 45 patents granted between June 2004 and July 2019.<sup>54</sup> Many of these were filed by STC and the SM Budyonny Academy, and some even list Tsarik and Terentiev as inventors alongside Shepilov. Shepilov also continued to appear on patents for STC and the SM Budyonny Academy after the founding of SMT-iLogic in 2015, including a patent granted in July 2018 for the invention of a ‘method and device for determining the coordinates of the source of radio-emissions’ that was tested with an Orlan-10.<sup>55</sup>

49 Stephen Grey, Maurice Tammam and Maria Zholobova, ‘The global supply chain feeding Russia’s killer drones’, Reuters, 15 December 2022.  
 50 Russian due diligence platform Excheck Pro notes that Tsarik and Terentiev were removed as company shareholders in August 2017. There is no mention of them being added to the company’s list of shareholders after it was founded, leading the authors to assume that they may have joined the company at the time it was established.  
 51 SMT-iLogic, ‘О компании’ [‘About the company’], <http://smt-ilogic.ru/>, accessed 14 November 2022.  
 52 Extract from the Unified State Register of Legal Entities of the Federal Tax Service of Russia LIMITED LIABILITY COMPANY ‘SMT-AYLOGIK’ as of 30 June 2017.  
 53 Эксчек Про [Excheck Pro], ‘ООО ‘СМТ-АйЛогик’ Хронология событий’ [‘LLC ‘SMT-iLogic’ Chronology of events’], <https://excheck.pro/company/7804552300/timeline>, accessed 15 November 2022.  
 54 A Google Patents search on 14 November 2022 for patents authored by Shepilov yielded 48 results, with some duplicates.  
 55 Александр Васильевич Золотов [Aleksandr Vasilevich Zolotov], Мария Васильевна Клестова [Mariya Vasilevna Klestova], Александр Владимирович Клишин [Aleksandr Vladimirovich Klishin], Мария Михайловна Липович [Mariya



Figure 4: Company Documents for SMT-iLogic Listing Terentiev and Tsarik

OFFICIAL SMT-ILOGIC COMPANY DOCUMENTS DATED 2017		ALEKSEI VASILIEVICH TEREITIEV LISTED AS COMPANY OFFICER																																													
<p>Выписка из ЕГРЮЛ ФНС России на 30.06.2017 ОГРН: 1157847407156</p> <p>Сведения о юридическом лице</p> <p><b>ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СМТ-АЙЛОГИК"</b></p> <p>ОГРН: 1157847407156 ИНН/КПП: 7804552300/780401001 по состоянию на 30.06.2017</p> <table border="1"> <thead> <tr> <th colspan="2">Наименование</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Полное наименование</td> </tr> <tr> <td>2</td> <td>Сокращенное наименование</td> </tr> <tr> <td>3</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> <tr> <th colspan="2">Сведения о состоянии юридического лица</th> </tr> <tr> <td>4</td> <td>Состояние</td> </tr> <tr> <td>5</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> <tr> <th colspan="2">Адрес (место нахождения)</th> </tr> <tr> <td>6</td> <td>Почтовый индекс</td> </tr> <tr> <td>7</td> <td>Субъект Российской Федерации</td> </tr> <tr> <td>8</td> <td>Улица (проспект, переулок и т.п.)</td> </tr> <tr> <td>9</td> <td>Дом (владение и т.п.)</td> </tr> <tr> <td>10</td> <td>Корпус (строение и т.п.)</td> </tr> <tr> <td>11</td> <td>Офис (квартира и т.п.)</td> </tr> <tr> <td>12</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> </tbody> </table>		Наименование		1	Полное наименование	2	Сокращенное наименование	3	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	Сведения о состоянии юридического лица		4	Состояние	5	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	Адрес (место нахождения)		6	Почтовый индекс	7	Субъект Российской Федерации	8	Улица (проспект, переулок и т.п.)	9	Дом (владение и т.п.)	10	Корпус (строение и т.п.)	11	Офис (квартира и т.п.)	12	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	<table border="1"> <thead> <tr> <th colspan="2">Сведения</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>ОГРН</td> </tr> <tr> <td>64</td> <td>ГРН и дата внесения в ЕГРЮЛ сведений о данном лице</td> </tr> <tr> <td>65</td> <td>Фамилия</td> </tr> <tr> <td>66</td> <td>Имя</td> </tr> <tr> <td>67</td> <td>Отчество</td> </tr> </tbody> </table> <p>Выписка получена через систему СПАРК (<a href="http://www.spark-interfax.ru">http://www.spark-interfax.ru</a>) Страница: 3</p>		Сведения		3	ОГРН	64	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице	65	Фамилия	66	Имя	67	Отчество		
Наименование																																															
1	Полное наименование																																														
2	Сокращенное наименование																																														
3	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
Сведения о состоянии юридического лица																																															
4	Состояние																																														
5	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
Адрес (место нахождения)																																															
6	Почтовый индекс																																														
7	Субъект Российской Федерации																																														
8	Улица (проспект, переулок и т.п.)																																														
9	Дом (владение и т.п.)																																														
10	Корпус (строение и т.п.)																																														
11	Офис (квартира и т.п.)																																														
12	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
Сведения																																															
3	ОГРН																																														
64	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице																																														
65	Фамилия																																														
66	Имя																																														
67	Отчество																																														
<p>Выписка из ЕГРЮЛ ФНС России на 30.06.2017 ОГРН: 1157847407156</p> <table border="1"> <tbody> <tr> <td>68</td> <td>ИНН</td> </tr> <tr> <td>69</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> </tbody> </table>		68	ИНН	69	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	<p>Выписка из ЕГРЮЛ ФНС России на 30.06.2017 ОГРН: 1157847407156</p> <table border="1"> <thead> <tr> <th colspan="2">Сведения</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>ОГРН</td> </tr> <tr> <td>82</td> <td>ГРН и дата внесения в ЕГРЮЛ сведений о данном лице</td> </tr> <tr> <td>83</td> <td>Фамилия</td> </tr> <tr> <td>84</td> <td>Имя</td> </tr> <tr> <td>85</td> <td>Отчество</td> </tr> <tr> <td>86</td> <td>ИНН</td> </tr> <tr> <td>87</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> <tr> <td>88</td> <td>Номинальная стоимость доли (в рублях)</td> </tr> <tr> <td>89</td> <td>Размер доли в процентах</td> </tr> <tr> <td>90</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> </tbody> </table>		Сведения		5	ОГРН	82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице	83	Фамилия	84	Имя	85	Отчество	86	ИНН	87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	88	Номинальная стоимость доли (в рублях)	89	Размер доли в процентах	90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																		
68	ИНН																																														
69	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
Сведения																																															
5	ОГРН																																														
82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице																																														
83	Фамилия																																														
84	Имя																																														
85	Отчество																																														
86	ИНН																																														
87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
88	Номинальная стоимость доли (в рублях)																																														
89	Размер доли в процентах																																														
90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
<p>Выписка из ЕГРЮЛ ФНС России на 30.06.2017 ОГРН: 1157847407156</p> <table border="1"> <thead> <tr> <th colspan="2">Сведения</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>ОГРН</td> </tr> <tr> <td>82</td> <td>ГРН и дата внесения в ЕГРЮЛ сведений о данном лице</td> </tr> <tr> <td>83</td> <td>Фамилия</td> </tr> <tr> <td>84</td> <td>Имя</td> </tr> <tr> <td>85</td> <td>Отчество</td> </tr> <tr> <td>86</td> <td>ИНН</td> </tr> <tr> <td>87</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> <tr> <td>88</td> <td>Номинальная стоимость доли (в рублях)</td> </tr> <tr> <td>89</td> <td>Размер доли в процентах</td> </tr> <tr> <td>90</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> </tbody> </table>		Сведения		5	ОГРН	82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице	83	Фамилия	84	Имя	85	Отчество	86	ИНН	87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	88	Номинальная стоимость доли (в рублях)	89	Размер доли в процентах	90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	<p>Выписка из ЕГРЮЛ ФНС России на 30.06.2017 ОГРН: 1157847407156</p> <table border="1"> <thead> <tr> <th colspan="2">Сведения</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>ОГРН</td> </tr> <tr> <td>82</td> <td>ГРН и дата внесения в ЕГРЮЛ сведений о данном лице</td> </tr> <tr> <td>83</td> <td>Фамилия</td> </tr> <tr> <td>84</td> <td>Имя</td> </tr> <tr> <td>85</td> <td>Отчество</td> </tr> <tr> <td>86</td> <td>ИНН</td> </tr> <tr> <td>87</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> <tr> <td>88</td> <td>Номинальная стоимость доли (в рублях)</td> </tr> <tr> <td>89</td> <td>Размер доли в процентах</td> </tr> <tr> <td>90</td> <td>ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения</td> </tr> </tbody> </table>		Сведения		5	ОГРН	82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице	83	Фамилия	84	Имя	85	Отчество	86	ИНН	87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	88	Номинальная стоимость доли (в рублях)	89	Размер доли в процентах	90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения
Сведения																																															
5	ОГРН																																														
82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице																																														
83	Фамилия																																														
84	Имя																																														
85	Отчество																																														
86	ИНН																																														
87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
88	Номинальная стоимость доли (в рублях)																																														
89	Размер доли в процентах																																														
90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
Сведения																																															
5	ОГРН																																														
82	ГРН и дата внесения в ЕГРЮЛ сведений о данном лице																																														
83	Фамилия																																														
84	Имя																																														
85	Отчество																																														
86	ИНН																																														
87	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														
88	Номинальная стоимость доли (в рублях)																																														
89	Размер доли в процентах																																														
90	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения																																														

Source: Russian Federal Tax Registry; graphic and annotation by RUSI OSIA.

These and other collaborations<sup>56</sup> suggest that Shepilov is closely connected to both STC and the Budyonny Academy and that he has continued to aid STC’s work on the Orlan-10 while being a shareholder of SMT-iLogic.

SMT-iLogic and STC are also linked through the address of a former STC subsidiary. In 2014, STC founded and took a 76% share in the now-liquidated Joint Stock Company Special Technologies Centre (JSC STC).<sup>57</sup> On corporate

documents, JSC STC listed its address as an office at 17 Nepokorenyh Prospekt in St Petersburg.<sup>58</sup> The address that SMT-iLogic lists on its website is a nearby unit in the same building.<sup>59</sup>

Significantly, this building also houses the Autonomous Non-Commercial Organisation of Continuing Professional Education Centre for the Training of Unmanned Systems Professionals (CP SBS).<sup>60</sup> Founded in August 2014, the CP SBS offers training on a range of matters related to UAVs,

Mikhajlovna Lipovich], Павел Леонидович Смирнов [Pavel Leonidovich Smirnov], Александр Михайлович Шепилов [Aleksandr Mikhajlovich Shepilov], Дмитрий Владимирович Царик [Dmitrij Vladimirovich Tsarik], , ‘Способ и устройство определения координат источника радиоизлучения’ [‘Method and device for determining the coordinates of the source of radio emission’], 2017, Russia Patent RU2659808C1.

56 Shepilov was a member of the SM Budyonny Academy’s teams that won awards for their inventions – including one team that invented a radio electronic complex for deployment on the Orlan-10. The team, which included Terentiev and Tsarik, won the gold medal at the 2015 ‘Archimedes’ International Invention and Innovative Technologies Salon in Moscow; Военная академия связи имени Маршала Советского Союза С.М. Буденного [SM Budyonny Military Academy of the Signal Corps], ‘Итоги участия изобретателей Военной академии связи на XVIII Московском международном салоне изобретателей и инновационных технологий «Архимед-2015»’ [‘Results of the participation of Military Academy of the Signal Corps inventors in the XVIII Moscow International Invention and Innovative Technologies Salon “Archimedes-2015”’], <<https://vas.mil.ru/folder/130585/item/6444>>, accessed 1 November 2022.

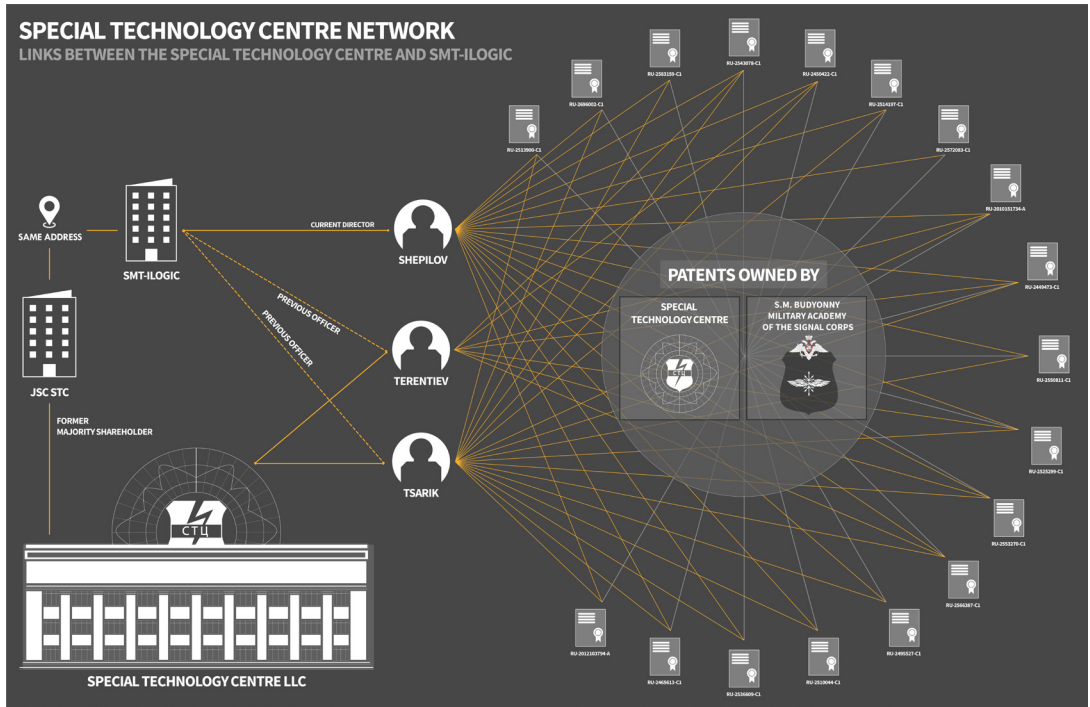
57 Original Russian text: Акционерное Общество ‘Специальный Технологический Центр’; INN: 7804531396; Russian Federal Tax Register, document dated 30 July 2020 from Sayari Analytics, <<https://sayari.com/>>, accessed 8 November 2022.

58 195220, город Санкт-Петербург, проспект Непокоренных, дом 17, корпус 4, литер В, помещение 3-Н, офис 214 [17 Nepokorenyh Prospekt, block 4, letter B, unit 3-N, office 214, St-Petersburg, 195220] (Russian Federal Tax Register, document dated 30 July 2022 from Sayari Analytics, <<https://sayari.com/>>, accessed 9 November 2022.

59 195220, город Санкт-Петербург, проспект Непокоренных, дом 17, корпус 4, литер В, помещение 5-Н [17 Nepokorenyh Prospekt, block 4, letter B, unit 5-N, office 214, St-Petersburg, 195220] (СМТ-АйЛогик [SMT-iLogic], ‘Контакты’ [‘Contacts’], <[http://smt-ilogic.ru/?page\\_id=21](http://smt-ilogic.ru/?page_id=21)>, accessed 11 November 2022).

60 Автономная некоммерческая организация дополнительного профессионального образования ‘Центр подготовки

Figure 5: STC and SMT-iLogic Connections



Source: Russian Patent Records; Sayari Analytics; graphic designed by RUSI OSIA.

Figure 6: An Orlan-10 at the CP SBS



Source: Image from website of CP SBS; annotations by RUSI OSIA.

including their operation and maintenance. Meanwhile, the Centre’s general director is Vasily Viktorovich Makarov,<sup>61</sup> who also served as general director and founding shareholder of JSC STC.<sup>62</sup> SMT-iLogic, as an undesignated entity,

was likely able to serve as a deniable vehicle for STC to procure microelectronics from suppliers located outside of Russia. To do so, it relied on a large, decentralised network of suppliers located in Europe, Asia and North America.

специалистов беспилотных систем’ (ЦП СБС); INN: 7804291271; ЦП СБС [CP SBS] ‘Контакты’ [‘Contacts’], <<https://cpsbs.com/contacts/>>, accessed 10 November 2022.

61 Василий Викторович Макаров; INN: 504503659986; ЦП СБС [CP SBS], ‘Руководство и педагогический состав’ [‘Management and teaching staff’], <<https://cpsbs.com/ob-ano/rukovodstvo-i-pedagogicheskij-sostav/>>, accessed 10 November 2022.

62 Russian Federal Tax Register, documents dated 18 December 2021 and 7 December 2019 from Sayari Analytics, <<https://sayari.com/>>, accessed 11 November 2022.



# Illicit Procurement

In February 2022, Florida resident Igor Kazhdan was indicted by the US government for procuring and shipping a wide range of export-controlled military and dual-use technologies to Russia.<sup>63</sup> Kazhdan, a dual citizen of Russia and the US, used the alias 'Alex Stanton' to operate two companies—IK Tech Corporation and GeoSat Microwave—in Dania Beach, Florida and California that advertised state-of-the-art commercial and military satellite technology.<sup>64</sup>

Kazhdan, however, was allegedly using his two companies to illegally procure export-controlled items for delivery to SMT-iLogic and another company based in St Petersburg named Device Consulting LLC.<sup>65</sup> Russian bank records confirm that STC has also paid millions of dollars to Device Consulting,<sup>66</sup> whose website—until recently—included a letter signed by 'Alex Stanton' certifying Device Consulting as an authorised distributor of GeoSat products.<sup>67</sup>

63 United States of America v. Igor Kazhdan, also known as 'Alex Stanton', 'Criminal Complaint', United States District Court for the Southern District of Florida, 0:22-mj-06066-PMH, 29 March 2022 see Pacer.gov, < <https://pacer.login.uscourts.gov/>>.

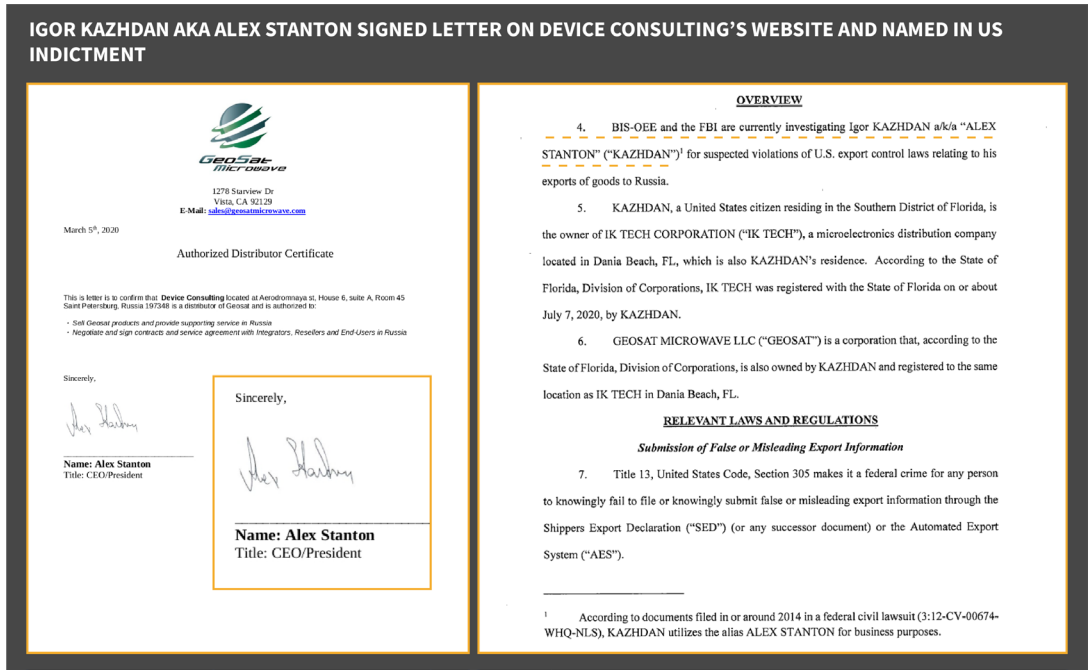
64 *Ibid.*

65 *Ibid.*

66 Stephen Grey, Maurice Tammam and Maria Zholobova, 'The global supply chain feeding Russia's killer drones', Reuters, 15 December 2022.

67 Девайс Консалтинг [Device Consulting], 'О компании' ['About the Company'], cached 27 May 2022, <<http://web.archive.org/web/20220527035255/https://device.consulting/about>>, accessed 28 November 2022.

Figure 7: Letter Signed by Alex Stanton AKA Igor Kazhdan on Device Consulting’s Website



Source: Documents found on www.Device.Consulting; United States of America v. Igor Kazhdan; annotations by RUSI OSIA.

The US indictment alleges that, between December 2021 and February 2022, Kazhdan acquired hundreds of export-controlled items from US-based manufacturers and fraudulently shipped them to Russia without a licence.<sup>68</sup> In December 2021, for example, Kazhdan allegedly procured over 100 power amplifiers with defence applications produced by US company Qorvo, which he then shipped to Device Consulting in Russia.<sup>69</sup> His company had also shipped Qorvo products to SMT-iLogic in April and June of the same year.<sup>70</sup> These Qorvo components are very similar to those found inside a captured Orlan-10.<sup>71</sup>

In fact, company-level shipment records filed between 2020 and 2022 confirm that Kazhdan’s companies exported large volumes of microelectronics to SMT-iLogic and Device Consulting, including critical components often used in the Orlan-10 that are also subject to US export controls.<sup>72</sup> Between October 2020 and February 2022, for example, IK Tech Corporation dispatched over 1,300 Gumstix-produced GUM3703FEBY computer-on-module units to both SMT-iLogic and Device Consulting.<sup>73</sup> This exact component was discovered in the payload control unit of an Orlan-10<sup>74</sup> and is also export-controlled by the US.<sup>75</sup>

68 Kazhdan indictment.

69 Specifically, 60 units of TGA2704-SM high-powered amplifiers and 40 units of QPA2211D Ka-band power amplifiers; Kazhdan indictment

70 Trade data supplied by third-party commercial provider.

71 Byrne et al., ‘Silicon Lifeline’.

72 Trade data supplied by third-party commercial provider.

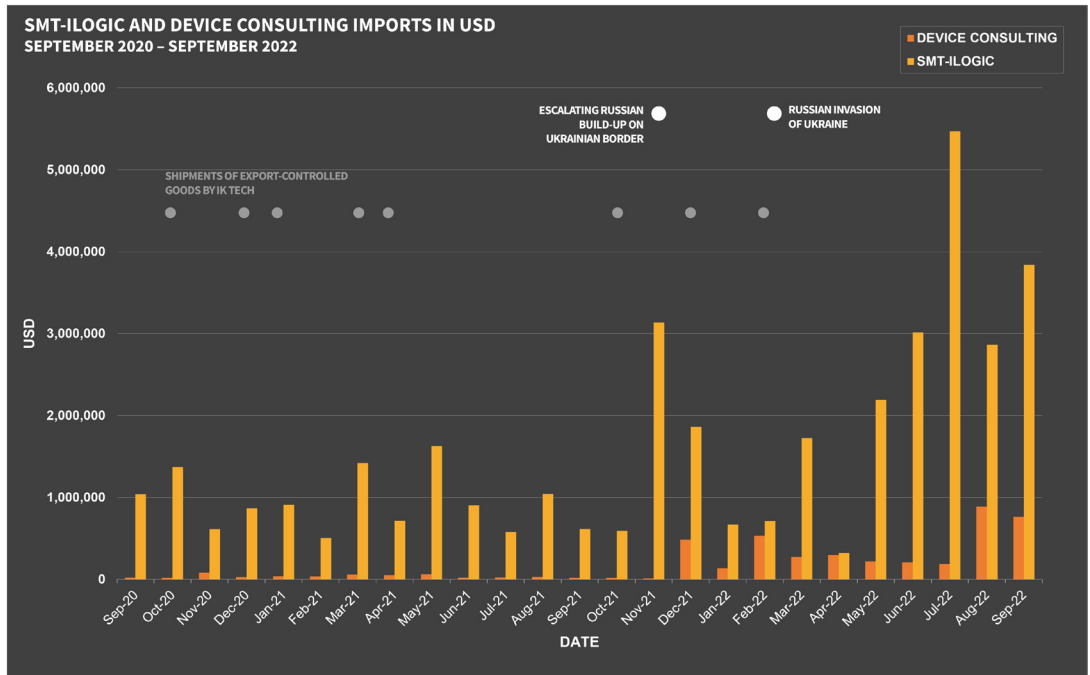
73 *Ibid.*

74 Byrne et al., ‘Silicon Lifeline’.

75 Mouser Electronics, ‘GUM3703FEBY’, <<https://www.mouser.ie/ProductDetail/Gumstix/GUM3703FEBY?qs=GBLSI2AkirtGRfvDUH%2Ffx8Q%3D%3D>>, accessed 15 November 2022. Mouser is an authorised distributor of this product; Gumstix, ‘Overo IronSTORM-BY COM’, <<https://www.gumstix.com/overo-ironstorm-by-com.html>>, accessed 9 November 2022.



Figure 9: SMT-iLogic and Device Consulting Import Timeline



Source: Russian Trade Data; Kazhdan Indictment, graphic designed by RUSI OSIA.

### CHINESE SUPPLIERS

Two of SMT-iLogic’s primary suppliers are Hong Kong-registered Xinghua Co Ltd<sup>84</sup> and Sinno Electronics Co Ltd, a US-designated<sup>85</sup> company previously identified by RUSI as shipping microelectronics to Russia to bolster the country’s defence industrial base.<sup>86,87</sup>

Xinghua began shipping to SMT-iLogic in December 2021 and has since become the company’s third largest supplier.<sup>88</sup> Shipment-level trade data states that Xinghua has been predominantly shipping portable computers

produced by Getac,<sup>89</sup> a Taiwanese manufacturer of rugged computers.<sup>90</sup>

The sole director and shareholder of Xinghua is a Chinese national named Yuan Jilun,<sup>91</sup> who is also the executive director and owner of Beijing-based Luchengtech Co Ltd,<sup>92</sup> a supplier of information technology products to China’s defence, aviation and space industries.<sup>93</sup>

84 Original Chinese text: 興華國際股份有限公司.

85 US Department of the Treasury, ‘Treasury Imposes Swift and Severe Costs on Russia for Putin’s Purported Annexation of Regions of Ukraine’, press release, 30 September 2022, <<https://home.treasury.gov/news/press-releases/jy0981>>, accessed 15 November 2022.

86 Byrne et al., ‘Silicon Lifeline’.

87 *Ibid.*

88 Trade data supplied by third-party commercial provider shows Xinghua Co Ltd accounts for 11% of SMT-iLogic’s imports from January to September 2022, since it began shipping to SMT-iLogic in December 2021.

89 Original Chinese text: 神基投控.

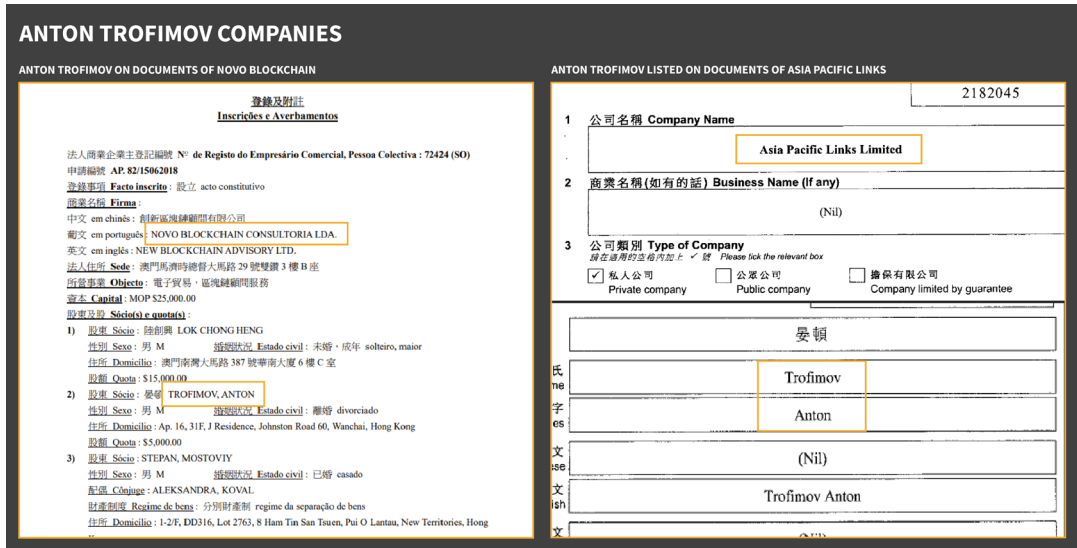
90 A rugged computer is a computer specifically designed to operate reliably in harsh usage environments and conditions. This may include the ability to withstand significant vibrations or extreme temperatures. See Getac, ‘About Us’, <<https://www.getac.com/en/about-us/>>, accessed 16 November 2022.

91 Original Chinese text: 袁继伦; Hong Kong Companies Registry, <<https://www.icris.cr.gov.hk/csci/>>, accessed 15 November 2022.

92 Original Chinese text: 北京兴华恒成科技发展有限公司; China National Enterprise Credit Information Publicity System, documents dated 19 December 2021 from Sayari Analytics, <<https://sayari.com/>>, accessed 16 November 2022.

93 Luchengtech, ‘Company profile’, <<http://en.luchengtech.com/intro/1.html>>, accessed 15 November 2022.

Figure 10: Companies linked to Anton Trofimov



Source: Hong Kong and Macao Companies Registries; annotations by RUSI OSIA.

Trade data also shows that Luchengtech shipped a range of goods to SMT-iLogic and Device Consulting in May, July and August 2022.<sup>94</sup> This included over 200 engines used in aviation modelling produced by Chinese companies DLE<sup>95</sup> and DTRC as well as data-processing and cloud-computing machines supplied by California-based Super Micro Computer Inc.<sup>96</sup> In addition, between 2019 and 2021, the company sold hundreds of Getac-made portable computers to SMT-iLogic.<sup>97</sup> This evidence of a relationship between these Chinese entities and AFRF-affiliated companies is particularly noteworthy, further highlighting the growing importance of Chinese companies to Russian military supply chains.<sup>98</sup>

**ANTON TROFIMOV**

However, by far the largest supplier to SMT-iLogic—accounting for 25% of imports in 2022—is Asia Pacific Links,<sup>99</sup> a Hong Kong-headquartered company owned and controlled by a Russian national named Anton Trofimov.<sup>100</sup>

Between 2019 and 2021, Asia Pacific Links shipped over \$10 million’s worth of microelectronic components to Russian companies, more than half of which were destined to SMT-iLogic and Device Consulting. After Russia’s February 2022 invasion, however, Asia Pacific Links appears to have increased deliveries, shipping over \$9 million of components to SMT-iLogic and Device Consulting alone.<sup>101</sup>

A number of these shipments appear to have contained a range of notable components. For example, between June and August 2022 Asia Pacific Links shipped at least 800 export-controlled quad-band cellular modules to the St Petersburg office of SMT-iLogic.<sup>102</sup> As noted above, these precise modules are often utilised in the Orlan-10. Other shipments in 2022 included components that have been found inside Orlan-10 UAVs, such as GNSS modules made by u-blox and computer-on-modules made by Gumstix.

94 Trade data supplied by third-party commercial provider.  
 95 The company also operates under the name Mile Hao Xiang Technology Co Ltd (弥勒浩翔科技有限公司). DLE, ‘Home’, <<https://www.dlengine.com/en/>>, accessed 23 November 2022.  
 96 Trade data supplied by third-party commercial provider.  
 97 *Ibid.*  
 98 Naomi Garcia, ‘Trade Secrets: Exposing China-Russia Defense Trade in Global Supply Chains’, C4ADS, 15 July 2022, <<https://c4ads.org/reports/trade-secrets/>>, accessed 9 November 2022.  
 99 Trade data supplied by third-party commercial provider.  
 100 Trofimov uses the Hong Kong address, Flat B, 2/F, Kar Yau Building, 36 Queen’s Road East, from Hong Kong Companies Registry, <<https://www.icris.cr.gov.hk/csci/>>, accessed 15 November 2022.  
 101 Trade data supplied by third-party commercial provider.  
 102 *Ibid.*

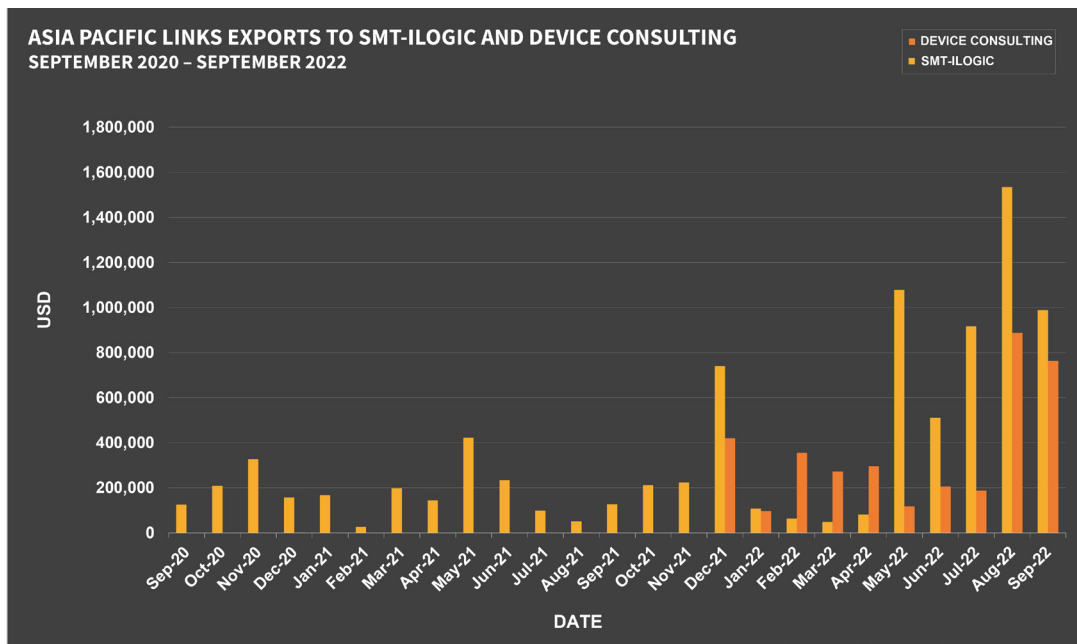
## Byrne, Bronk, Watling, Somerville, Byrne and Baker

Trofimov, who founded Asia Pacific Links in 2014, operates a number of other companies in Canada, China, Hong Kong and Macao.<sup>103</sup> His LinkedIn profile also claims that he has been involved with the GP Gentlemen’s Club at the Tigre de Cristal Hotel and Resort, based just outside Vladivostok,<sup>104</sup> since April 2019.<sup>105</sup>

However, another one of Trofimov’s companies, the Macao-registered New Blockchain Advisory,<sup>106</sup>

also appears to have shipped large quantities of microelectronic components and semiconductors to Device Consulting,<sup>107</sup> the St Petersburg company that received shipments from Kazhdan.<sup>108</sup> One of these shipments, made in 2021, reportedly included over \$6,000 of direction-finding compasses manufactured by Safran Sensing Technologies,<sup>109</sup> whose products are advertised for military and UAV applications.<sup>110</sup>

**Figure 11: Asia Pacific Links Exports to SMT-iLogic and Device Consulting**



Source: Russian Trade Data; graphic designed by RUSI OSIA.

103 Sayari Analytics, <<https://sayari.com/>>, accessed 15 November 2022; Hong Kong Companies Registry, <<https://www.icris.cr.gov.hk/>>, accessed 15 November 2022.

104 Муравьиная Бухта, 73. Артем, Приморский край [Muravjinaya Bay, 73. Artyom, Primorsky Krai.

105 LinkedIn, ‘Anton Trofimov’, <<https://ca.linkedin.com/in/anton-trofimov-89823b36/>>, accessed 14 November 2022.

106 Original Chinese text: 創新區塊鏈顧問有限公司, also known as Novo Blockchain Consultoria Lda; Macao Commercial Registry Office, documents dated 15 June 2018 from Sayari Analytics, <<https://sayari.com/>>, accessed 11 November 2022.

107 Trade data supplied by third-party commercial provider.

108 Kazhdan indictment.

109 As of October 2021, the company became a subsidiary of Safran Electronics & Defense, <<https://www.sensor.com/about/news/change-of-ownership/>>, accessed 10 December 2022.

110 Safran Sensing Technologies, <<https://www.safran-group.com/companies/safran-sensingtechnologies>>.



# Conclusion

The Orlan-10 is one of Russia's most essential and indirectly lethal pieces of military equipment, and one that relies on Western components for a significant number of its critical functions. The Russian military is urgently attempting to increase the number of Orlan-10s available for artillery-spotting, reconnaissance, EW and SEAD/DEAD duties in Ukraine as both sides make preparations for renewed offensive operations in spring 2023.<sup>111</sup>

The production quantities required to increase numbers while also replacing combat losses implies a continued requirement for large volumes of components to be brought in through the networks identified in this report. Disrupting these networks should, therefore, be considered a high priority for Western efforts to counter sanctions evasion, since reducing the number of Orlan-10s available to the Russian military by spring 2023 would significantly reduce overall force lethality and give the Ukrainian military more room for manoeuvre.

Russian missile and aircraft manufacturing practices require many new components to be thoroughly tested and certified as safe in operation with all the other elements of each system. This also applies to some of the components that might be introduced as substitutes for Western-supplied ones in the event of a successful embargo. This process of certification – putting aside the development time to find and fit new components – is assessed to take three months, each time a change is made to the design.<sup>112</sup> Hence, even if Russia were able to find technically viable substitutes for many of the Western components identified in this report, integrating them into the Orlan-10 production line would create major delays, add cost and thus help buy time for Ukrainian forces. In some cases, replacing these Western-manufactured components will be impossible in the short run.

However, as detailed in this report, Russian companies closely associated with the manufacturer of the Orlan-10 have been able to increase imports

of necessary components since the beginning of the invasion. Given that much of this technology is ultimately manufactured and produced by companies domiciled in Western states, greater effort should be made to prevent diversion to Russia's military manufacturers by intermediaries in the US, Europe, Hong Kong and China.

To do so, governments should act against those individuals and entities responsible for diverting components to the AFRF and step-up efforts to monitor their flow to important transshipment-hubs and suspicious third parties. Governments should also improve guidance and expand capacity building activities for the private sector and financial institutions in countries that are often exploited by those seeking to procure technology for the AFRF.

## AUTHORS

**James Byrne** is the Director of Open-Source Intelligence and Analysis (OSIA) at RUSI.

**Jack Watling** is Senior Research Fellow for Land Warfare at RUSI.

**Justin Bronk** is a Senior Research Fellow for Air Power at RUSI.

**Gary Somerville** is a Research Fellow in OSIA at RUSI.

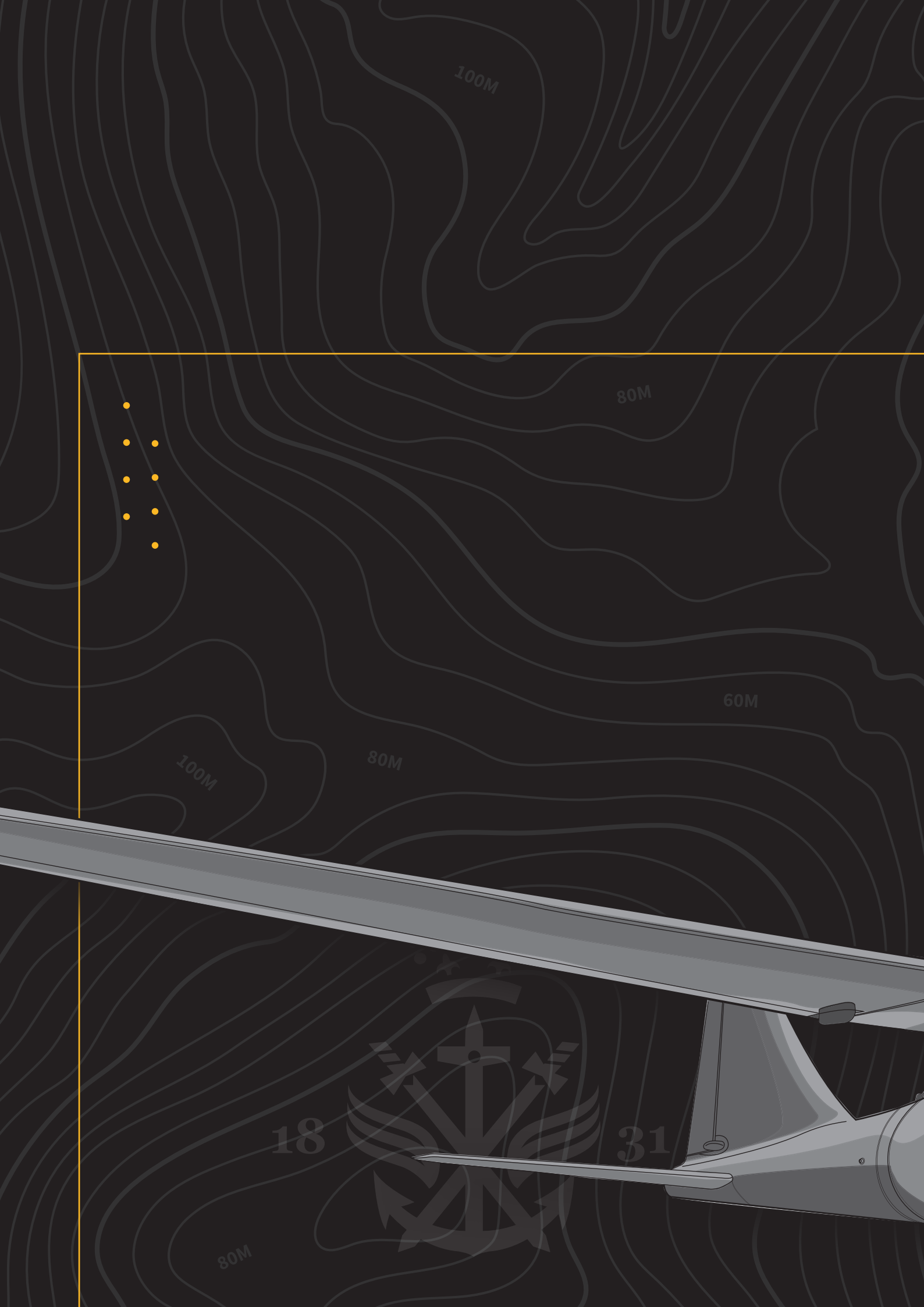
**Joe Byrne** is a Research Fellow in OSIA at RUSI.

**Jack Crawford** is Research Analyst in OSIA at RUSI

**Jane Baker** is an independent consultant.

<sup>111</sup> Author fieldwork in Ukraine.

<sup>112</sup> Byrne et al., 'Silicon Lifeline'.



100M

80M

60M

100M

80M

18

31

80M

