Women In International Security

POLICYbrief

WIIS POLICYbrief May 28, 2020

WEB | www.wiisglobal.org

EMAIL | info@wiisglobal.org

1301 Connecticut Avenue NW, Suite 750
Washington, D.C. 20036

# *NATO and 5G: Managing "High Risk" Vendors and Other Outsourced Infrastructure*

**Clodagh Quain and Isabelle Roccia**

Fifth-generation telecommunications (5G) technology promises to dramatically increase the interconnectedness and efficiency of commercial and civilian communication infrastructures. 5G will also enable other advances. On the civilian side, it will improve existing applications and give rise to others, from telemedicine to connected cars. It also presents an opportunity to enhance NATO's capabilities, improving logistics, maintenance, and communications. For instance, 5G will speed communication and improve response time in a theater of operation.

These developments also pose challenges. 5G is part of a complex architecture. To leverage its full benefits, millions of sensors and devices will need to be deployed and connected, from smart home appliances and connected toys to full-scale factories and critical infrastructures. The number of connected devices is projected to total 41.6 billion worldwide by 2025.[1] By 2030, this estimate ratchets up to 125 billion.[2] Of these, mobile devices will grow from 8.8 billion in 2018 to 13.1 billion devices by 2023 – 1.4 billion of which will be 5G capable.[3] Because devices are connected to one another or to a network, security risks will multiply. The Alliance faces an increased challenge in ensuring that NATO Allies' 5G networks and the critical infrastructures that rely on them can withstand multiple physical and cybersecurity threats.

NATO's main concern in this context is the risk associated with foreign ownership or management of critical infrastructure, including by private operators and foreign state actors in supply chains. That such ownership could result in collusion between the supplier and a country's intelligence or security services is deemed particularly worrisome by many governments, critical infrastructure operators and industry alike.[4] For NATO allies, supply-chain risk management is therefore a critical aspect of the strategic and operational challenges posed by 5G.

At the NATO meeting in London in December 2019, Allies prioritized 5G security as part of its security and resilience agenda. The final declaration stated, "NATO and Allies, within their respective authority, are committed to ensuring the security of our communications, including 5G, recognizing the need to rely on secure and resilient systems."[5] Including 5G in the London Declaration formalized NATO's work in this emerging field.

## *Background*

5G technology is transformative on several fronts. It will challenge the design and implementation of existing infrastructure and applications. The velocity and pervasiveness of 5G technology will stimulate development of advanced applications, including smart cities and autonomous vehicles.

A diverse set of suppliers form the 5G ecosystem, which encompasses network infrastructures, spectrum, devices and software. While Ericsson (Sweden), Nokia (Finland)

and Huawei (China) are the three best-known vendors, they represent only a small number of the stakeholders involved. The telecommunications industry estimates that operators will have to invest $1.1 trillion by the end of 2025 to build 5G networks.[6]

In 2016, the European Commission developed a 5G Action Plan for Europe to support launching the rollout of commercial 5G services in all EU member states by the end of 2020.[7] Subsequently, there will be a rapid buildup of infrastructure in urban areas and along major transport routes by 2025.[8]

At the Prague 5G Security Conference in May 2019, 32 EU and NATO members adopted recommendations known as the Prague Proposals.[9] They propose principles that governments should apply to 5G deployment, stipulating that communication networks and services should be "designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best practices." State representatives also called for the adoption of principles of fairness, transparency, risk-based policy and interoperability.

## *Relevance for NATO*

Since 1949, NATO has centered on safeguarding the security and freedom of its members. Its mandate has evolved in political and geographic terms as the world changed. Today, emerging technology, with its many political, military and commercial implications, is driving NATO's need to adapt.

Given its broad membership overlap with the European Union, deployment of 5G in Europe will undoubtedly affect the Alliance. The implications for NATO allies are strategic and operational in nature and affect defensive and offensive postures. At a minimum, dependence on 5G exposes critical infrastructure to more vulnerabilities, including software vulnerabilities, which NATO allies must address.[10] That said, 5G can also improve capabilities such as communication security.[11]

At the multilateral level, NATO, like the European Union, seeks to balance collective and national interests. At the Munich Security Conference on February 15, 2020, NATO Secretary General Jens Stoltenberg referred to guidelines and basic requirements that both organizations had developed for infrastructure investment—notably in telecommunications and 5G.[12]

On January 29, 2020, the Network and Information Systems (NIS) Cooperation Group published an EU toolbox, with measures to mitigate risks identified in the EU coordinated risk assessment report of October 9, 2019:

- strategic measures on regulatory powers for incident reporting, security measures, threats and assets;
- initiatives to promote a diverse supply and value chain;
- technical measures to strengthen the security of networks and equipment; and
- risk mitigation plans.[13]

NATO's leadership also seeks to develop a minimum set of common practices for resilient telecommunications while avoiding encroachment on individual state approaches. At the October 2019 NATO Defense Ministerial meeting, for example, representatives agreed to update the baseline requirements for civilian telecommunications, including 5G.[14] This update covered foreign ownership, foreign control and direct investment. While civilian infrastructure remains a "national responsibility," Article 3 of NATO's founding treaty states that resilience, intended to prevent the failure of critical infrastructure or hybrid attacks, is part of states' commitments to the Alliance and to one another. The Secretary General reiterated NATO's approach the following month at the NATO Industry Forum in Washington, DC, where he linked resilience of supply chains and that of nations and the Alliance.[15]

NATO members maintain the right to decide national policies for regulating critical infrastructure and 5G vendors. For example, UK Foreign Secretary Dominic Raab addressed the House of Commons on January 28, 2020, outlining the government's review of national telecommunications and its position on "high risk vendors." The United Kingdom approved the use of equipment acquired from "high risk vendors" while restricting those vendors' access to "safety critical networks."[16] The foreign secretary stressed that the review would not hamper his government's ability to share sensitive data with its partners over highly secure networks. In May 2020, the UK Government decided to review the impact of the decision on national networks with the assistance of the National Cyber Security Centre.

## *What Is at Stake?*

Foreign ownership or management of critical infrastructure is a significant risk for NATO allies. Consequently, more governments may look to adopt procurement rules that limit sourcing to trusted vendors.

Such a position creates another risk, however. Indeed, the operators of critical infrastructure may have only limited capacity to detect, prevent and recover from the cybersecurity risks they face if they cannot choose the technologies and processes they need to match security requirements stemming from their size, complexity and risk profile. These operators must remain in control of how they improve their overall security posture if they are to meet the security and resilience objectives set nationally or at NATO.

Innovation with state-of-the-art technology is critical in the interconnected environment in which Allies find themselves, through cross-border infrastructure (for energy supply, for instance) or shared functions (such as airspace control). NATO's value-added in this context is to facilitate the development and sharing of baseline requirements for supply-chain risk management among Allies. It can also be to share best practices and information on risks and threats. This coordination would ensure that all individual state efforts contribute to more secure, resilient critical infrastructures.

## Recommendations

As NATO allies move forward, they should focus on four main issues: leveraging NATO and EU membership, assessing supply-chain management issues, adopting a principled approach and building international consensus.

*Leveraging Membership*: 5G affects strategic, political, industrial and commercial elements on both sides of the Atlantic. The integrated economies of the European Union and the United States share a common value system, with policies that traditionally align with NATO's, despite conflicting messages from the current US administration regarding its commitment to the Alliance. Despite the inherent cross-border, integrated nature of critical infrastructure in Europe, EU member states approach supply-chain evaluation differently. As the European Union seeks a coordinated, harmonized process for 5G supply-chain assessment, it is important that NATO and the EU align their policies in this regard. The lack of such alignment might create challenges for NATO, such as overdependence on one supplier.

*Supply-Chain Risk Management:* NATO allies must consider the global, interconnected nature of supply chains and the threats they face as they weigh effective approaches to 5G supply-chain risk management. Their approaches should ultimately strengthen NATO's strategic mission, inform procurement guidelines and harmonize risk-management baselines across Allies. Such risk management entails identifying likely threats, vulnerabilities and potential consequences, tailoring mitigation strategies to risks and prioritizing actions based on an assessment of the most relevant, potentially impactful risks.[17]

*A Principled Approach:* A similar or harmonized set of principles should underpin effective supply-chain risk management. These principles should do the following:

- encourage interoperability of systems and the use of state-of-the-art technologies;
- ensure, where possible, transparency of supply-chain risk management policies and their implementation, in part to facilitate best practices;
- develop a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats;
- collaborate with key nongovernmental stakeholders, including industry, to adapt to an ever-changing environment of new technologies and new threats;
- invest in research and development of new technological approaches to fostering supply-chain integrity; and
- avoid prohibiting the acquisition or integration of some technologies simply because they were developed abroad.

*Building International Consensus*: Several international organizations and groups have begun to assess the 5G environment and its related security risks. The Prague 5G Repository produced a library of tools, frameworks and legislative measures to assist NATO member states. Multilateral organizations, such as the EU, and states have come to similar conclusions. They too underline major risks that have national security implications. Integrity, confidentiality and availability of networks and communications are also key to their security.

## Conclusion

5G innovation is not just a technological choice but a strategic one. Even in a collective defense system such as NATO, states remain sovereign, making decisions based on their assessment of the geopolitical environment. A state approach driven primarily by economic opportunity may undermine collective defense and security.

To both build and manage 5G capabilities, NATO's allies will need to leverage EU and NATO membership; balance national and collective methods for supply-chain risk management; apply a principled approach to supply-chain integrity; and coordinate at the state and international levels.

Former director of Carnegie Europe Tomáš Valášek referred to critical civilian networks as "the path of least resistance" for adversaries in the digital age to divide NATO from within.[18] To protect this critical infrastructure, he argues, both the public and private sectors will need to invest in IT expertise. This shared challenge presents an opportunity for NATO and other multilateral organizations to fill gaps for their member states and to adapt to emerging technology beyond their traditional role. It is a novel test for NATO: to broker strategic geopolitical rivalries and national security concerns over critical infrastructure while developing its own modern capabilities and addressing the multiple fractures in global and allied security today.

## References


1. International Data Corporation (IDC), The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, press release (Framingham, MA: IDC, June 18, 2019).

2. IHS Markit, *The Internet of Things: A Movement, Not a Market*, presentation (London: IHS Markit, 2017), p. 2.

3. Cisco, *Annual Internet Report (2018–2023),* white paper (San Jose: Cisco, 2020), p. 2.

4. Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, *Huawei, 5G, and China as a Security Threat* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019).

5. NATO, London Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London 3-4 December 2019, press release (Brussels: NATO, December 4, 2019).

6. GSMA Intelligence, *The Mobile Economy 2020* (London: GSM Association, 2020), p. 5.

7. European Commission, *5G for Europe: An Action Plan,* COM(2016) 588 final (Brussels: European Commission, 2016), p. 4.

8. European Commission, Future Connectivity Systems, *5G for Europe Action Plan* (Brussels: European Commission, December 19, 2019).

9. Government of the Czech Republic, Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals, press release, May 3, 2019.

10. Flexera, *Vulnerability Review 2018: Global Trends* (Itasca, IL: Flexara Software LLC, 2018).

11. Karl Norrman, Prajwol Kumar Nakarmi, and Eva Fogelström, *5G Security—Enabling a Trustworthy 5G System,* Ericsson White Paper (Stockholm: Ericsson, January 8, 2020).

12. NATO Secretary General Jens Stoltenberg, Transcript of Opening Remarks, Munich Security Conference, Brussels, February 15, 2020.

13. European Commission, *Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures* (Brussels: European Commission, January 29, 2020).

14. NATO Secretary General Jen Stoltenberg, Press Conference Following the Meeting of NATO Defense Ministers, Brussels, October 25, 2019.

15. NATO Secretary General Jens Stoltenberg, Keynote Address at the NATO Industry Forum, Washington DC, November 14, 2019.

16. United Kingdom, Foreign Secretary's Statement on Telecommunications, London, UK Foreign Secretary Office, January 28, 2020.

17. BSA | The Software Alliance (BSA), *BSA Principles for Good Governance: Supply Chain Risk Management* (Washington, DC: BSA, 2019).

18. Tomáš Valášek et al., "NATO at 70: What Next?" *Politico* (April 3, 2019).


## Authors


**Clodagh Quain** is Policy Analyst at the Institute of International and European Affairs (IIEA), Dublin, Ireland. The views expressed here are those of the author and not of the IIEA.

**Isabelle Roccia** is Senior Manager, Policy - EMEA at BSA | The Software Alliance in Brussels, Belgium.

This publication is the result of a joint WIIS DC, WIIS Brussels, WIIS France, and WIIS UK project focused on new challenges for the NATO alliance and showcasing the expertise of the Next Generation women defense experts. Through a competitive selection process six Next Generation experts were invited to participate in programs on the sidelines of the 2019 December NATO Leaders meeting. We would like to thank our six experts for their thoughtful contributions to this initiative, WIIS Global for publishing their research and the US Mission to NATO for providing the generous grant without which this project would not have been possible. With this support, we were able to turn an idea to promote greater cooperation among our affiliates and cities into a reality. We hope this project encourages more collaboration across borders and helps bolster the overall WIIS mission of supporting women in the international security field.

The NATO Consortium Team: Michelle Shevin-Coetzee, WIIS-DC; Armida van Rij, WIIS UK; Florence Fernando and Pauline Massart, WIIS Brussels; Ottavia Ampuero and Jessica Pennetier, WIIS France.

WIIS DC
WOMEN IN INTERNATIONAL SECURITY

wiis WOMEN IN INTERNATIONAL SECURITY BRUSSELS

WIIS
Women In International Security France

WIIS Women in International Security United Kingdom

## RECENT WIIS PUBLICATIONS

POLICYbrief

Chantal de Jonge Oudraat and Michael E. Brown, *The Gender and Security Agenda: Strategies for the 21st Century* (London: Routledge, June 2020)

Kulani Abendroth-Dias and Carolin Kiefer, *Artificial Intelligence is Already Transforming the Alliance: It is Time for NATO and the EU to Catch Up*, WIIS Policy Brief (May 2020)

Nad'a Kovalčíková and Gabrielle Tarini, *Stronger Together: NATO's Evolving Approach toward China,* WIIS Policy Brief (May 2020)

Shannon Zimmerman, *The Value of a Feminist Foreign Policy*, WIIS Policy Brief (February 2020)

Sarah Kenny, *Women of the Alt-Right: An Intersectional Study of Far-Right Extremism, Gender, & Identity in the United States*, WIIS Policy Brief (August 2019)

Pearl Karuhanga Atuhaire & Grace Ndirangu, *Removing Obstacles to Women's Participation at the Peace Table and in Politics*, WIIS Policy Brief (March 2019)

Chantal de Jonge Oudraat & Soraya Kamali-Nafar, *The WIIS Gender Scorecard: Washington, DC Think Tanks*, WIIS Policy Brief (September 2018)

Pearl Karuhanga Atuhaire & Grace Ndirangu, *Sexual and Gender Based Violence in Refugee Settings in Kenya and Uganda*, WIIS Policy Brief (June 2018)

Luisa Ryan & Shannon Zimmerman, *Gender Parity in Peace Operations: Opportunities for US Engagement*, WIIS Policy Brief (June 2018)

Velomahanina T. Razakamaharavo, Luisa Ryan, & Leah Sherwood, *Improving Gender Training in UN Peacekeeping Operations*, WIIS Policy Brief (May 2018)

Spencer Beall, *Missing Figures: The Cybersecurity Gender Gap*, WIIS Working Paper (May 2018)

Chantal de Jonge Oudraat and Michael E. Brown, *WPS+GPS: Adding Gender to the Peace and Security Equation*, WIIS Policy Brief (November 2017)

Hamoon Khelghat Doost, *Women in Jihadist Organizations: Victims or Terrorists?*, WIIS Policy Brief (May 2017)

Jeannette Gaudry Haynie and Chantal de Jonge Oudraat, *Women, Gender, and Terrorism: Understanding Cultural and Organizational Differences*, WIIS Policy Brief (April 2017)

Ellen Haring, *Equipping and Training Modifications for Combat Arms Women*, WIIS Policy Brief (January 2017)

Fauziya Abdi Ali, *Women Preventing Violent Extremism: Broadening the Binary Lens of "Mothers and Wives,"* WIIS-HoA Policy Brief (February 2017)

Jeannette Gaudry Haynie and Chantal de Jonge Oudraat, *Women, Gender, and Terrorism: Policies and Programming*, WIIS Policy Brief (January 2017)

Jeannette Gaudry Haynie, *Women, Gender, and Terrorism: Gendered Aspects of Radicalization and Recruitment*, WIIS Policy Brief (September 2016)

Antonieta Rico and Ellen Haring, *Combat Integration Handbook: A Leader's Guide to Success* (September 2016)

Chantal de Jonge Oudraat and Michael E. Brown, *Women, Gender, and Terrorism: The Missing Links*, WIIS Policy Brief (August 2016)

Chantal de Jonge Oudraat, Sonja Stojanovic-Gajic, Carolyn Washington and Brooke Stedman, *The 1325 Scorecard: Gender Mainstreaming Indicators for the Implementation of UNSCR 1325 and its Related Resolutions* (Brussels,Washington, DC and Belgrade: NATO-SPS Programme, WIIS and Belgrade Centre for Security Policy, October 2015)

Ellen Haring, Megan MacKenzie and Chantal de Jonge Oudraat, *Women in Combat: Learning from Cultural Support Teams*, WIIS Policy Brief (August 15, 2015)

*WIIS Policy Roundtables and Policybriefs are supported by the Embassy of Liechtenstein in Washington, DC.*

*WIIS Next Generation efforts are supported by Carnegie Corporation of New York.*



## ABOUT WIIS

Women In International Security (WIIS) is the premier organization in the world dedicated to advancing the leadership and professional development of women in the field of international peace and security. WIIS (pronounced "wise") sponsors leadership training, mentoring, and networking programs as well as substantive events focused on current policy problems. WIIS also supports research projects and policy engagement initiatives on critical international security issues, including the nexus between gender and security.

To learn more about WIIS and become a member, please visit http://wiisglobal.org/.

WIIS
WOMEN IN INTERNATIONAL SECURITY