No. 115
September 2019

SECURITY POLICY BRIEF

Security aspects of connectivity

Tomas Ries

Published in October 2018, the European Commission's joint communication Connecting Europe and Asia – Building Blocks for an EU Strategy offers a good outline of the principles underlying the European Union's (EU) connectivity interests. However, the document does not address the security implications of connectivity: it merely notes that "'flow security' matters". This Policy Brief attempts to cover that gap and expand on the notion of flow security. Security challenges should not be seen as an intrinsic obstacle to connectivity itself, or to its development. What we call "connectivity" today is part of a deeper trend whereby societies and economies are increasingly tied to each other, and most developed economies now bid on a further deepening of this trend, as is apparent in discussions over the "internet of things" (IoT) or "Industry 4.0". Still, connectivity entails specific and dynamic challenges that require dedicated attention

Background - Basic Implications of Connectivity

Connectivity refers to all the ways in which states, organisations (commercial or else) and societies are connected to each other and interact across the globe. This includes both the physical flows of people and goods as well as information flows. Connectivity is a property (of being connected or interconnected), not a policy. It covers "hard" infrastructures as well as "soft" regulatory measures or socio-cultural ties. As such, it can foster flows of all kinds: increased trade for instance, or tourism, or K-pop music; but also illegal trades, greater information sharing among terrorist groups, pollution or diseases.

Connectivity and flow security are particularly relevant in today's world since global connectivity and interactions have expanded and intensified massively over the last thirty years. For instance, "the number of active mobile-broadband subscriptions have increased from 268 million in 2007 to 5.3 billion in 2018"[1] . Today almost every state in the world depends on huge flows of goods, capital, data, people, technology and ideas.

As connectivity increases, so does the need to secure these many flows from serious disruptions. The concept of "flow security"

introduces the notion that security is not only tied to the protection of a particular entity, territory or population; the protection of flows, and the critical infrastructure (including service providers) on which they rely, require dedicated attention and resources. For interconnected societies and economies, the challenge is existential.

Like all things, connectivity has both positive and negative security implications. The deepest positive security impact of connectivity arises when growing interconnectedness and interdependence leads to a convergence of views and interests among parties. When all parties see a benefit in it, then connectivity fosters security[2]. This process can even upgrade a peaceful connectivity relationship into a deeply shared vital interest for all parties. Such a 'positive sum' relationship, and its deep mutual dependencies, strongly inhibits conflict and war among members, as long as all parties perceive that the benefits of cooperation greatly exceed those of confrontation. These processes also justify the creation and upholding of common rules or international regimes. This logic was indeed one of the founding principles of the European Coal and Steel Community, and it remains an important pillar of the EU as a European 'peace project' today. The EU has even staked much of its history and added value on the "four freedoms": the guarantee of a free movement of goods, capital, services, and labour.
Further indirect security benefits of connectivity include enhanced competition among economic units, greater information exchange among societies and an overall drive to innovate for companies and societies alike.

The deepest negative security impact of connectivity relates to the potential consequences of dependence: what effects could a partial or total breakdown in connectivity have on a society and economy? Connectivity makes all parties much more vulnerable to regional or global volatility or turmoil. A related problem is that dependencies also create vulnerabilities that can be used to exert coercion. Asymmetry in dependence, as can be the case between a big and a small economy, plays to the benefit of the least dependent. Dependence in strategic sectors, for instance in the supply of rare earth minerals or 5G technology, while environmentally or economically sound, can have adverse security implications.

A second challenge is that connectivity also requires societies to be competitive in terms of productivity (work ethic, education, creativity, entrepreneurial spirit, etc.). This is good per se, but if significant parts of society are unable to compete they may turn against connectivity. What we see happening in large parts of Europe (Brexit, anti-migrant policies in Hungary, etc.) and in the United States (Trump's protectionist platform) today demonstrates how connectivity, its policy agenda and its consequences, can mobilize voters around populist ideas and exclusionary policies.

A fine balance must thus be maintained between pursuing the cooperative benefits of connectivity and avoiding the potential vulnerabilities and domestic tensions that it can engender.

STATE OF PLAY - SECURITY CHALLENGES OF CONNECTIVITY

Two basic types of security challenge emerge with connectivity. One consists of the dangers from connectivity itself. The second consists of the dangers to connectivity, or more specifically to the hard and soft infrastructure on which connectivity depends.

CHALLENGES FROM CONNECTIVITY

The danger from connectivity consists of the vulnerabilities noted above. Dependence on

external flows has been multiplied with the introduction of hyper-effective technical and economic systems. The decreasing cost of movement allowed companies to decentralize their supply chains, optimize product flows and spend ever less on storage. Global just-in-time delivery services mean that most advanced economies today have very few buffers or reserves. Several European economies depend upon global deliveries of vital commodities on a 24-hour basis: in case of a serious disruption of these critical supplies, stocks would run short in a day. In 2011, catastrophic floods in Thailand, where many subcontractors in the chip and automotive industry were based, dramatically impacted the production of personal computers and cars at a global level[3] . The same applies to services and critical infrastructure: for instance, a recent World Bank report on logistics performance found that supply chain reliability and service quality are strongly associated with logistics performance[4] .

The societies of most small and medium-sized states today depend entirely on the constant flow of global supplies for their food, energy and jobs. In most cases there are no buffers and no reserves. This leaves very little resilience should the global flows break down. One basic, and largely overlooked, challenge arising from connectivity is how to combine global functional integration with national resilience so that connected societies can survive in case of disruptions. Measures to promote resilience can either be national (yesterday's model), regional (for instance mutual assistance agreements within the EU) or global (the multilateral agenda).

CHALLENGES TO CONNECTIVITY

The second set of security challenges is the vulnerability of the flows themselves. These challenges are many and they can require very specific expertise and policies to address, but it is useful to categorize them in three broad dimensions: the political, functional and ecological.

Political challenges to connectivity: Connectivity faces two sorts of political challenges. One consists of 'external' hostile actors attacking connectivity directly. This constitutes the "geopolitics of connectivity". The second consists of 'internal' hostile actors attacking connectivity indirectly. This is rather related to the "politics of connectivity".

Today, the geopolitics of connectivity convoke three types of actors: transnational revolutionary movements (transnational terrorism), organised crime and states. The three differ in terms of motivation and capability.

Transnational terrorism movements, such as Al Qaida or ISIS, could be highly motivated to break down parts of national or global flow systems. Targeting critical infrastructure such as airports or nuclear power plants, poisoning water supplies, hacking financial systems and the like could inflict a serious blow to their main enemies and carry an important symbolic charge. However, their capacity to carry out debilitating attacks on critical systems is more limited than the other two.

Organised crime is not motivated to disrupt flows; on the contrary it profits from them. The problem here is that its activities are so harmful to societies (corruption, drugs, extortion) and industry[5] . Currently they are primarily a source of serious friction and corrosion but do not present an existential threat. However, they could, if motivated, marshal considerable resources given their massive financial resources.

Then comes the states themselves, as geopolitical actors with high capacity and ever-increasing

stakes in connectivity affairs. Most states with the resources to break down critical flows are also dependent upon them. Total disruption is hardly an option for any of them, unless attacked, but we have already seen a number of limited "flow attacks" against individual states, either at a low level (economic sanctions) or against small targets (the Russian denial-of-services attack on Estonia in 2007).

As connectivity deepens and widens, including in the cyber domain, so does the portfolio of actions available to states in pursuit of their national interests. For instance, network resilience in the face of cyber-attacks and/or attacks on critical infrastructure (e.g. satellites) is a major concern for modern armed forces. It so appears that connectivity can be challenged in "abnormal conditions", as in the event of escalating confrontation or open conflict between major powers, or in very specific conditions, as when a state decides that losses incurred in a domain (impairing connectivity) can be outweighed by gains in another (electoral platform, military resilience, etc.).

To illustrate this second condition, it is useful to mention the Russian military's approach to connectivity. The Russian conception of war focusses heavily on functional attacks directed against the economic and technical systems of adversaries. This was clearly outlined by the Chief of the Russian General Staff General Gerasimov in a 2012 article[6] . The focus is on 'breaking the internal coherence of the enemy system', which means disrupting the societies, economies and technical infrastructure of potential adversaries. Gerasimov notes that the correlation between these measures and the use of outright military force is 4:1. In other words breaking the social and functional base has four times as much effect as military force. Furthermore, there are ample signs showing that Russia is applying principles of this "functional war" against the EU and United States at the present. Particularly disturbing in the functional context are the signs of a sustained Russian effort to penetrate our information systems[7] , and the systematic Russian naval activity focused on the undersea cables connecting the world wide web[8].

The "politics of connectivity" is less about foreign policy, more about the relationship between state and society when connectivity reinforces or creates socio-economic lines of fracture. In the EU and the United States, where a significant share of voters is reacting against rising unemployment, declining real incomes and a decline in public services, the "social contract" increasingly emerges as a potential casualty of connectivity. Attacks on representative democracy are a component of this changing political landscape but contending approaches toward connectivity are another: the Brexit campaign and Trump's slogans similarly targeted flows of people as a danger to the nation, requiring effective action and a partial shutting down of particular flows.

Functional Challenges to Connectivity: Functional challenges to connectivity do not include hostile actors, but consist entirely of technical problems in the design, maintenance and management of the economic and technological systems on which our societies depend. In a fast-changing technological environment – think 5G technology, Artificial Intelligence, etc. - this is a critical issue. It is also where we have faced (or thought so) at least two existential challenges since the end of the Cold War.

The first possible near meltdown was the Y2K syndrome. This emerged as we approached the new millennium and became aware of the danger that computer operating systems might shut down when their datelines showed only zeros at

the turn of the century. We will never know if this was a real danger or not because we spent billions of dollars and human resources trying to prevent it. In the event nothing happened, but had it taken place it could have shut down the world as we know it. This is a clear example of how a pure design flaw could lead to a catastrophe.

The second near catastrophe was Wall Street in 2008, when the global financial system suffered a near meltdown. In this case the problem was not a design flaw but mismanagement, as those responsible took too many risks, and the bubble burst. Had governments not saved their banks, the result might have been an economic crisis of considerably higher proportions than has been the case. Such is, at least, the contention of the economic and political actors most involved at the moment.

Maintenance entails challenges of its own. Electricity grids, land communications, information networks, etc. require regular maintenance and modernisation. They may be vulnerable to man-made and natural disasters. They can suffer from inadequate supporting services. In a long-term perspective, maintaining and modernizing one's critical infrastructure requires strategic planning, including for instance the choice of particular standards in next generation equipment or the selection of foreign partners based on more than simply economic and industrial considerations.

Ecological Challenges to Connectivity: Ecological challenges to connectivity include all natural events that could damage or break global social and functional flows. The most severe potential danger is the possibility of a major pandemic. This could choke the free movement of goods and people, effectively shutting down global physical connectivity. Other examples include natural disasters, such as the tsunami in 2011 that knocked out the Japanese nuclear plant at Fukushima. This in turn not only led to a serious radiation leak, but also to some 25% of Japanese electricity production being lost. This forced factories to shut down, which in turn broke global supply chains of sub-components, which in turn affected industrial production across the globe. There are a host of other such ecological challenges that could affect global functional flows.

PROSPECTS

Connectivity raises three broad security challenges and a host of specific sub-challenges, some of which are outlined above. In terms of policy agenda, there are three broad lines of action available to governments that would support a strategic approach toward connectivity.

First, establishing a new social contract in our societies. In an interconnected world, the nationally delimited systems of political representation and the architectures of wealth redistribution are under considerable pressure. New options should find a way to balance the intense competitive demands on individuals in connected economies against the need to provide livelihood means for the segments of the population deemed most likely to suffer from global competition and economic transformation. The alternative is likely to be a continuous rise of populist narratives and policies.

Second, increasing the resilience of our states and societies on an individual basis and collectively as part of the EU, should connectivity flows be disrupted. Critical first measures include raising the awareness of this sort of challenge among decision-makers, mapping our vulnerabilities and identifying existing and desired responses. More concrete options include: further integrating energy grids, allowing breaks in one part of the EU to be compensated for from others; establishing joint fire-fighting units that can be

sent to stricken areas as needed (we already have rudimentary arrangements to this end); establishing central stockpiles of vital commodities such as fodder or seed, and so forth. This is where the EU can play a crucial role, since it can develop more cost-effective responses and avoid duplication.

Third, ensuring the security of the connectivity flows themselves, which involves protecting their supporting hard and soft infrastructure from the myriad political, functional and ecological stresses they are vulnerable to, and which will likely increase in coming decades.

Addressing these challenges is as important as promoting connectivity. A first step could be to launch a coordinated research effort focussed on the concept of flow security and its applicability to the EU context. This would be a natural topic for the EU, as a possible addition to its recently launched "connectivity strategy" and a welcome clarification of how it intends to engage with the challenges and opportunities of the global connectivity debate.

Dr. Tomas Ries is Senior Lecturer (Assistant Professor in the US) in Security and Strategy at the National Defence College, Stockholm, Sweden

ENDNOTES

[1]"ITU releases 2018 global and regional ICT estimates", ITU *Press Release*, 7 December 2018: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx

[2]See for instance: WRIGHT, Robert, *Nonzero: The Logic of Human Destiny*. New York: Vintage Books, 2000, 435 p.; SLAUGHTER, Anne-Marie, *The Chessboard and the Web: Strategies of Connection in a Networked World*. New Haven and London: Yale University Press, 2017, 304 p.; WOLF, Martin, *Why Globalisation Works*. New Haven and London: Yale University Press, 2004, 398 p.

[3] Ploy Ten Kate and Chang-Ran Kim, "Thai floods batter global electronics, auto supply chains", Reuters, 28 October 2011:https://www.reuters.com/article/us-thai-floods/thai-floods-batter-global-electronics-auto-supply-chains-idUSTRE79R0QR20111028

[4] The World Bank, *Connecting to Compete 2018 Trade Logistics in the Global Economy*. Washington D.C.: The World Bank, 2018: http://documents.worldbank.org/curated/en/576061531492034646/pdf/128355-WP-P164390-PUBLIC-LPIfullreportwithcover.pdf

[5]See for instance the World Atlas of Illicit Flows at: https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION.pdf or LALLERSTEDT, Karl: "Measuring Illicit Trade and its Wider Impact." In: Virginia COMOLLI (ed.), *Organized Crime and Illicit Trade*. London: Palgrave MacMillan, 2018, pp. 79-110.

[6]GERASIMOV, Valery, (Charles BARTLES transl.) "The Value of Science is in the Foresight", *Military Review*, Jan-Feb 2016: pp. 23-29. Available here: https://jmc.msu.edu/50th/download/21-conflict.pdf

[7]See for instance: *Threat Assessment 2018*. PST. Norwegian Police Security Service Annual Report. Available here: https://www.pst.no/globalassets/artikler/trusselvurderinger/annual-threat-assessment-2018.pdf

[8]See for instance: MacASKILL, Ewen, "Russia could cut off internet to NATO countries, British military chief warns", *The Guardian*, 14 December 2017: https://www.theguardian.com/world/2017/dec/14/russia-could-cut-off-internet-to-nato-countries-british-military-chief-warns