Parsing Pegasus

An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics

Leander, Anna

Document Version
Accepted author manuscript

Published in:
Swiss Political Science Review

DOI:
10.1111/spsr.12441

Publication date:
2021

License
Unspecified

Citation for published version (APA):
Leander, A. (2021). Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics . *Swiss Political Science Review*, *27*(1), 205-213. https://doi.org/10.1111/spsr.12441

Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics

Abstract: How do technologies matter for security politics? This article introduces the kind of arguments an *infrastructural approach* would focus its answer on. It illustrates how the approach would work by focussing on how the spyware Pegasus developed by the Israeli company NSO matters for Swiss security politics. It follows the infrastructural approach showing how and why it would tend to three things primarily: the politics of the *infrastructures* Pegasus is inscribed in, the politics of the processes of *infrastructuring* the software generates and the *infrapolitics* that sustain and transform these processes and infrastructures. The article also discusses the strengths and weaknesses of infrastructural approaches, underlining that since they are relational, processual and radically open epistemologically and ontologically, infrastructural approaches are suitable for opening new agendas, re-problematising and re-imagining the politics of security technologies. They are less suited for studies premised on a fixed understanding of the politics of security technology.

Zusammenfassung: Welche Verbindung besteht zwischen Technologie und Sicherheitspolitik? Dieser Artikel zeigt, wie ein infrastruktureller Ansatz uns hilft, Antworten zu formulieren. Es werden drei Schlüsselkonzepte des Ansatzes vorgestellt (*infrastructure, infrastructuring* et *infrapolitics*). In Bezug auf die Kontroverse um die Pegasus-Software, die von der israelischen Firma NSO verkauft wird, zeigt er, wie diese Konzepte dazu beitragen, die politischen Fragen der Technologie für die Sicherheitspolitik zu verstehen. Der Artikel hervorhebt, den Unterschied ein infrastruktureller Ansatz gegenüber einem traditionelleren Ansatz zentriert beispielsweise auf die Strategien und Interessen der Akteure oder das geopolitische Gleichgewicht.

Résumé: Quel est le lien entre la technologie et la politique de sécurité ? Cet article montre comment une approche infrastructurelle nous aide à formuler des réponses. Il introduit trois concepts clés de l'approche (*infrastructure, infrastructuring* et *infrapolitics*). Avec référence à la controverse concernant le logiciel Pegasus vendu par la firme Israélienne NSO, il montre comment ces concepts permettent de comprendre les enjeux politiques de la technologie pour la politique de sécurité en insistant sur la différence qu'une approche infrastructurelle fait par rapport aux approches plus traditionnelles centrées p.ex. sur les stratégies et intérêts des acteurs ou l'équilibre géopolitique.

Keywords: New materialism, Military Markets, Commercial Security, Affect, Aesthetics

Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics

Pegasus is the mythical winged white horse of Greek mythology, fathered by Poseidon and foaled by Medusa when Perseus decapitated her. Pegasus could travel impossible distances to unreachable places and help achieve the unachievable. Pegasus is also a program that makes it possible to bypass the *WhatsApp* encryption. It is developed, marketed and sold by the Israeli NSO Group. It is a spyware. This Pegasus became a scandal when it was revealed that Saudi Arabia had used it to gather information about the Saudi journalist Khashoggi, later murdered in Istanbul. Pegasus also became a scandal in Switzerland when, in the wake of the international debate around it, the spyware showed up on Swiss phones.[1] Throughout the international scandals surrounding the spyware, the NSO Group affirmed that Pegasus was only sold to customers who would use it ethically, for defensive purposes, in the fight against violence and terrorism. The NSO Group's assertions were backed up by the Israeli government, whose export regulations the sales of Pegasus had to adhere to. As it turned out, the sale of Pegasus to Saudi Arabia had been approved in the process associated with these regulations.

Pegasus the spyware, as Pegasus the mythical white horse, travelled impossible distances, to the unattainable place of *WhatsApp* and helped listen in on encrypted inaccessible conversations. Pegasus is a technology that matters for security politics generally, and for Swiss security politics specifically. But *how* does it matter? One family of answers — perhaps the dominant one? — would look at who has used Pegasus, for what purposes and what the implications of this were for Swiss politics. This is also how the connection between technology and security politics is often approached: technology is a tool. Its political significance depends on who uses it, how, against whom. Here I draw attention towards another family of answers that focuses on how technology itself is political and is doing politics. Pegasus is not merely a tool (which obviously it also is) but a political 'actant' that matters for security politics. Below I introduce one branch of this family of approaches: the infrastructural one. I do so in a threefold argument delineating the main building blocks and rationale of this approach:

The first part introduces the basic contention of this approach, which is that politics is located in the mundane, aesthetic/affective and emerging socio-material *infrastructures*. To assess the significance of Pegasus for security politics on this account therefore requires looking beyond the noisy scene of scandal politics towards the invisible work done in the infrastructures underpinning it. The second part directs attention to the multiplicity of *infrastructuring* processes in which politics is enacted (and infrastructures reproduced), emphasising the import of a focused, critical but also constructive

---

[1] The term paper and documentary made by Severin Ruoff and Mona Zimmermann (2019) for the IHEID Master in International Affairs class *The Politics of Commercial Security* offers a a good inroad to this discussion argument. For a summary of their contribution see https://graduateinstitute.ch/communications/news/business-privatised-espionage (accessed 16 January 2021).

engagement. To get a grasp of and intervene with how Pegasus does security politics, we need to focus attention, critically and constructively, on the processes through which it comes to matter. The third, final part of this threefold introduction outlines the reasons infrastructural approaches are necessarily tied to an *infrapolitics* probing the boundaries that underpin infrastructures by keeping the curious at a distance. Parsing the significance of Pegasus for security politics through an infrastructural approach requires giving up on the security of safely bounded academic and professional turfs and the policing that goes into securing them. In the conclusion, I return to the relation between this infrastructural approach and other approaches to technology and Swiss security politics.

Infrastructures

That infrastructure matters to politics is no news. Most disciplines have had their own version of an interest in the infrastructures of politics. Recently however, infrastructural studies have received renewed attention as scholars interested in various forms of new materialism in a wide range of different disciplines have come to see infrastructures as offering an inroad to capturing material politics, including the politics of technology. In approaches that grapple with digital politics, the turn to infrastructure has been particularly pronounced (Bowker 2014). The core contention of infrastructural approaches is that politics are increasingly enacted in — and prefigured by — socio-material infrastructures. On this account, the significance of Pegasus for security politics lies in the 'invisible work' of infrastructures (Star and Strauss 1999) that makes *WhatsApp* conversations, their encryption and the hacking of this encryption central to security politics (and not in the scandals that this politics gives rise to). Three central characteristics of infrastructural work make its politics particularly salient and elusive.

First, infrastructural work is mostly *mundane* and seemingly apolitical. In digital infrastructures, it is decentered, distributed and technical. It revolves around cables, switches, protocols, and technical standards designed by engineers and programmers as well as around internet users whose postings, commenting, flagging, linking and clicks are a form of digital labour (Van Dijck 2009). However, perhaps because of the absence of centralized authority, the political significance of this mundane digital infrastructural work and its role in governance are widely recognized. Internet governance is depicted as 'protocol politics' and a governance '*by* [not of] infrastructure' involving a wide range of heterogenous actors and technologies (DeNardis 2009; DeNardis and Musiani 2016; also Dunn Cavelty and Egloff 2021). Mundane infrastructural worked mattered for Pegasus. While obviously states (the Israeli and the Swiss among many) were involved in tampering with the technology, the core of the political agency rested with the commercial strategies of private companies, centrally the NSO Group and *WhatsApp*, the encryption standards developed by engineers, and the way these had come to shape social media communication.

Second, infrastructures work as much through *affective / aesthetic resonance* with our senses as through reflected reasoning. Infrastructures create 'atmospheres' that sensitize us to the world in one way rather than another. The design of urban infrastructures shapes security affectively (as also discussed by Hagmann and Kostenwein 2021). In digital infrastructures, the technical affordances of meditated communication shift the form of politics. Compare the politics of Trump's tweeting or of company advertising to conventional political debate. The images and sounds are far more central than in conventional politics. Digital infrastructures register and adjust what we are shown and relate to it in ways that feed into our affective and habitual political communication (e.g. Chun 2016). Exploring the politics of Pegasus from this perspective sensitizes us to this affective and aesthetic infrastructural work. It encourages us to focus e.g. on the (affective) trust placed encrypted groups assumed to be shielded from the intrusion of business or the pictures of oppression or ironic memes (aesthetic form) central to communication in these groups. The trust Khashoggi placed in *WhatsApp* and the form his communication there were conditions of possibility for his arrest by the Saudi authorities and the Pegasus scandal unfolding from that arrest. Infrastructural approaches direct attention to them.

Third, infrastructural work is not fixed and unchanging but *constantly morphing*. Even the effects of solid and firm bridges in New York, Russian pipelines or the electric grid in Palestine are constantly changing. They prefigure politics but politics is inscribed in them and transforming them in turn (Ballon and Jackson 2007, Barry 2013, Shamir 2013). This *emergent* character of infrastructures marks also digital infrastructures. They are partly 'self-organising systems', with emergent qualities that make them more fluid than fixed (also Wenger and Fischer 2021). Code, protocols and standards are rewritten. Software and hardware are reconfigured. Actors and norms shift. Digital infrastructures configure constellations of constantly evolving temporalities, or what Gumbrecht (2014) terms versions of our 'broad present'. The emergent character of digital infrastructures directs attention to the unstable, contextual, open relationship between technologies, such as Pegasus, and security politics. In so doing, it also highlights the import of acknowledging this openness analytically when studying the relations between technology and security politics, and politically when reflecting on the implications of these analyses for the possibility of intervening with and fashioning these relationships. This leads to how approaching the relationship between technology and politics in terms of infrastructures can help us gauge their significance.

Infrastructuring

Assessing the significance of Pegasus and other technologies by locating them in the mundane, aesthetic/affective, and emergent infrastructures of which they are part and through which their politics is done is a first step. It takes us to the question of how they do this. What are the precise processes through which politics is enacted? What links the anchoring of a technology in infrastructures to political outcomes? Or, what is the infrastructuring at work? To begin providing an

answer, one would have to decide what kind of *politics* and what kind of infrastructuring *process* one would be interested in.

For politics, one might for example take an interest in the infrastructuring of subjects and hence agency. Following a Foucauldian line one might look at how infrastructuring generates subjectivation or the "choreographing of impressionable subjects" (Introna 2017). Alternatively, adopting a Bourdieu inspired approach one might instead look at the infrastructuring of relational positions and dispositions of actors in a given field (Couldry 2004). Or, drawing on Mol's focus on the (ontological) 'politics of what', one might explore the infrastructuring of multiple political subjectivities. For infrastructuring process, one might decide to focus for example on the place of the algorithmic decision in making the infrastructures and the way it generates e.g. anomalies, the way it forms understanding of content, including images, or the way it organizes circulation (Gillespie 2018). This obvious need to choose, and therefore also to make explicit the choices made, is a strength in working with infrastructural approaches to security. These options and the necessity to choose among them, remind us that there are always a plurality of possible questions to ask of politics but no unique overarching, transcendental criteria for deciding which one to focus on. It is a 'critical choice' reflecting an 'Erkenntnisinteresse'.

A critical choice also needs to be made with regards to which kinds infrastructuring processes to focus on. There are at least two options for how to proceed. On the one hand, infrastructuring is often approached 'critically' directing attention to processes infrastructuring domination. For example, the hegemonic visibility sustaining social, racial, gendered or post-colonial identities works through the infrastructuring of 'data shadows' and the 'yearning or potential' to be seen that "become ever more pronounced in the face of unfulfilled promises of 'comprehensiveness' and 'completeness' of 'big data' in digital infrastructures" (Leonelli et al. 2017: 193). The aim of such critical approaches to infrastructuring is usually to identify possibilities to resist or disrupt the status quo. On the other hand, infrastructuring can also be approached constructively (Austin and Leander 2021). One could imagine constructively engaging with the design of infrastructures; designing infrastructuring to rearrange certain (racial, gendered, social, or colonial) hierarchies. For example, it may be possible to re-design at least some of the 'dangerous liaisons' between political authority, technical expertise, and financial interests that can be prejudicial for citizens, to make them work instead to their benefit (Musiani 2013). Some politics may be anchored so deeply and affectively anchored in digital infrastructures that it cannot be redesigned. The internet depends on a political subject that can be impressed and ever more deeply so. The commercial exercise of branding is not only etymologically associated with the branding of cattle and slaves (Introna 2017). The marks of branding go even deeper and go inside, below the skin, into the body and our imaginaries (Leander 2019)? Not everything can be redesigned.

The critical and constructive paths for following infrastructuring processes are therefore not opposites. Rather, they crisscross and overlap in ways that generate a "certain balance" between a politics intent on "defeating the existing order, and a politics aimed at providing an alternative to the political order" (Hage 2012: 292). This is also how they serve as exploration of the relationship between Pegasus and

security policy. Critique leads to a tracing of the infrastructuring of domination through the spyware operating e.g. through its pricing, the Israeli or more generally Zionist values embedded in it, or the kinds of political communication bubbles it affords. Construction opens for an exploration of the imaginations that rely on infrastructuring to produce an alternative order e.g. by shifting the pricing structure, delink Pegasus from the values associated with them, or shifting the communication bubbles it affords. The multiplicity of institutions, companies, internet activists and academics vying to transform the digital infrastructuring of politics points to the third and last part of this threefold argument introducing an infrastructural approach to the relation between Pegasus and security politics. It directs attention to centrality of 'infrapolitics' necessary for any engagement with infrastructures and infrastructuring.

Infrapolitics

Infrapolitics is a term that has been used to capture the politics of intervening with infrastructures and infrastructuring processes. Infrapolitics takes place outside and away from the formal political sphere. It is politics of hidden dissent or resistance (Scott 2005). It is also a creative politics "premised on the infra, that is the underlying rules of the world, organized around glocal infrastructures" (Thylstrup 2019: 25). The last point I will make is that infrastructural approaches depend on an academic infrapolitics of sorts to be feasible that defies the policing of disciplinary boundaries and make space for work across them.

Pegasus the spyware, the infrastructure that makes it significant and the infrastructuring through which this significance is enacted, transgress many of the basic distinctions organising both academic thinking and socio-material practice. For example, but by no means exhaustively, this includes the basic boundaries separating the socio/material, aesthetic/mundane, public/private, national/international, or civilian/military. This multiple and complex boundary crossing has far-reaching implications. The boundaries frame how we conceptualize, problematize and engage with the world as scholars of various disciplines. They are also practical categories, inscribed in the socio-material arrangements governing not only academic research but also the remit of competencies of states, international organizations and NGOs, as well as regulatory and political forms and fora. These boundaries are therefore hard and well policed. Perhaps for good reason. The distinctions ensure that each academic discipline and profession focuses on 'what it is best at'. Lawyers who logically are more competent in law can focus on regulation, while security specialists can delve into the risks etc.

However, for gauging the significance of Pegasus (or technology more generally) for Swiss security politics from an infrastructural perspective, this common-sense affirmation of boundaries becomes deeply problematic in at least two ways. First, it chops up the infrastructure/-ing and the responsibility for engaging with it. In so doing, it also makes it impossible to see the connections from which much of the significance of something like the Pegasus spyware derives. With the division of academic labour among specialisms, the overall picture disappears. The forest is lost for focus on the trees, the

infrastructure for its components. The intertwining of technology, aesthetics, law, affects, economics and security in the infrastructures and infrastructurings that makes Pegasus significant for Swiss security policy disappear from view. Second, and consequently, falling back on common-sense boundaries moves the responsibility for engaging with the infrastructures and infrastructuring elsewhere (not necessarily conspiratorial or even reflected). Legal scholars invoke the expertise of engineers who call on risk analysts who place it on the table of the media analysts etc. If everyone shoves responsibility elsewhere, it ends up nowhere. Falling back on basic categories therefore makes the significance of infrastructures not merely difficult to see but also something no one wants to see, or has the responsibility to look at.

The academic boundaries are backed up by the role of boundaries in practice: the NSO Group's insistence that it is only a company, acting according to prevailing Israeli laws is a way of policing the boundaries for engaging with it. It can be engaged with in terms of economics and Israeli law, not in terms of the more serious questions the case also rather obviously raises about political rights and freedom of expression, relations between intelligence policy and commercial interests, questions of race, gender and class, or privacy protection. Academics, the representatives of institutions, governments and activists act analogously and with similar consequences, when they mobilize the categories that delineate the boundaries of their respective turfs, denying responsibility for and interest in engagement with something like Pegasus beyond these.

An infrapolitics countering the problematic effects of common-sense boundaries is therefore a necessary part of any infrastructural approach. Called for is a politics revolving around the basic boundaries underpinning infrastructures, an engagement with what Bourdieu would have termed 'the category effects' underpinning and reproduced through infrastructures. Such a politics must necessarily be resolutely opposed to the policing of these borders, an 'anti-consensus politics' directed at the 'conceptual infrastructures' of research (Rancière 2008; Strathern 2018). It may be important to emphasize that this infrapolitics does not reject or deny the significance of common-sense borders. On the contrary, infrapolitics matters because of its attentiveness to them. It invites us to follow the infrastructures and infrastructuring in their transgressions of these boundaries and to explore the significance of these transgressions. To do so competently requires collaborations and alliances. It requires making oddkin— that is becoming kin with the odd, i.e. the out of place and bizarre (Haraway 2016). For IR and security studies scholars, trespassing the boundaries of the own turf by making kin with legal theorists, the ICANN or the ministry of defence is likely to seem odd. Doing so with encryption specialists, the NSO Group account manager, the director of the Technology and Human Rights section of Amnesty International or an analyst from MELANI[2] is likely to seem even more so. Yet, to gauge the significance of Pegasus (or other technologies) and reflect on how to intervene with

2 The Swiss agency responsible for coordinating cybersecurity.

it, such trespassing may be necessary, not only 'interesting'. Infrapolitics is necessary to make it imaginable, and hence possibly feasible, to do this.

Conclusion

In this contribution to our debate about technology and Swiss security policy, I have introduced an infrastructural approach. I have briefly delineated its claims that we would do well to focus on the mundane, aesthetic/affective and emergent infrastructures that the technology is part of and enacted through; that we need to work selectively, critically and constructively with the infrastructuring of politics and that to do this requires a micro-level, constructive, anti-policing infrapolitics. I have made this argument drawing on Pegasus, showing how an infrastructural approach would engage in parsing the significance of this Israeli spyware. A short discussion contribution, such as this one, obviously has to stop at outlining basic features and contours of this parsing, pointing to its possible variants. The substantive empirical and conceptual work of parsing Pegasus (and other technologies) is ahead. This contribution is an invitation to do it and some pointers to where to begin.

The contribution conveys enough about the core features of infrastructural approaches to indicate how they relate to politics and in what ways this relationship is different from that of other approaches. Infrastructural approaches are relational, processual and radically open epistemologically and ontologically. Their approach to analysing the relationship between technology and security politics is therefore one geared primarily understanding the dynamics of this relationship. Infrastructural approaches are suitable for providing pictures, opening new agendas, re-problematising and reimagining politics. This may be helpful for professionals such as diplomats, company leaders, activists, academics and others interested in gaining a grasp of, reframing and intervening with the security politics of technology and doing so realistically. However, this makes infrastructural approaches ill-suited for consultancy work, aimed at solving predefined problems. They will seem a distracting, cumbersome, annoying detour to those who have reached certitude about the relation between technology and security politics. For them, the infrastructural approach just outlined would provide marginal background knowledge at best. However, is such certainty and the accompanying closure warranted? The *Cunning of Uncertainty* at the heart of contemporary knowledge practices makes it appear misplaced generally (Nowotny 2016). The uncertainty about the politics of a decentralized, rapidly changing, complex digital environment — such as that of the Spyware Pegasus — makes it appear even more so.

Acknowledgments

Thanks to Myriam and Jonas for convening this discussion and for constructively commenting on (and helping me cut) previous versions of this contribution. Thanks also Dagmar Rychnovska and Luisa Lobato for their comments on earlier versions of the argument and the students in my IHEID course

The Politics of Commercial Security for discussing most of these ideas. The arguments remain mine of course and I would make them differently today. The first version of this contribution was submitted in the summer 2019 and much has changed since then.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Biography

Anna Leander is Professor of International Relations at the Graduate Institute in Geneva and at the PUC, Rio de Janeiro. She is best known for her practice theoretical contributions and her work on the politics of commercial security. Her current research focuses on international politics of design. Email: anna.leander@graduateinstitute.ch

Bibliography

Austin, J.L. and A. Leander (2021). Designing-with/in World Politics. *Forthcoming* under review.

Ballon, H. and K. Jackson (2007). *Robert Moses and the Modern City: The Transformation of New York*. WW Norton & Company New York.

Barry, A. (2013). *Material Politics: Disputes Along the Pipeline*. Hoboken: John Wiley & Sons.

Bowker, G. (2014). Foreword: The Infrastructural Imagination. In: Mongili, A and G. Pellegrino (eds.) *Information Infrastructure(s): Boundaries, Ecologies, Multiplicity*. Cambridge: Cambridge Scholars Publishing, (1-12).

Chun, W. (2016). *Updating to Remain the Same: Habitual New Media.* Cambridge: MIT Press.

Couldry, N. (2004). Theorising Media as Practice. *Social semiotics* 14 (2):115-32.

DeNardis L. (2009). *Protocol politics: The globalization of Internet governance.* Boston: MIT Press.

DeNardis, L. and F. Musiani (2016). Governance by Infrastructure. In: F. Musiani, L. Cogburn, L. DeNardis, et al. (eds.) *The Turn to Infrastructure in Internet Governance*. Houndsmill and New York: Palgrave-Macmillan, (3-24).

Dunn Cavelty, M. and F. Eggloff (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. *Swiss Political Science Review* 27(1): XXX-XXX.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. New Haven: Yale University Press.

Gumbrecht, H. (2014). *Our Broad Present: Time and Contemporary Culture*. New York: Columbia University Press.

Hage, G. (2012). Critical Anthropological Thought and the Radical Political Imaginary Today. *Critique of Anthropology* 32 (3):285-308.

Hagmann, J., and D. Kostenwein (2021). Urban Design as Technology of Security Politics. *Swiss Political Science Review*. 27(1): XXX-XXX.

Haraway, D. (2016). *Staying with the Trouble: Making Kin in the Chthulucene*. Duke: Duke University Press.

Introna, L. (2017). Die Algorithmische Choreographie Des Beeindruckbaren Subjekts. In Seyfert, R. and J. Roberge, *Algorithmuskulturen. Über Die Rechnerische Konstruktion Der Wirklichkeit*. Bielefeld: Kulturen der Gesellschaft, Band 26 (41-74).

Leander, A. (2019). Sticky Politics: Composing Security by Advertising Tracking Devices. *European Journal of International Security* 4 (3): 322-344.

Leonelli, S., B. Rappert and G. Davies (2017). Data Shadows: Knowledge, Openness, and Absence. *Science, Technology, & Human Values* 42 (2):191-202.

Musiani, F. (2013). Dangerous Liaisons? Governments, Companies and Internet Governance. *Internet Policy Review* 2 (1): 1-7.

Nowotny, H. (2016). *The Cunning of Uncertainty*. Oxford: Polity Press.

Rancière, J. (1998). *Aux Bords Du Politique*. Paris: Gallimard.

Scott, J. (2005). The Infrapolitics of Subordinate Groups. In Amoore, L. (ed.) *The Global Resistance Reader*. London and New York: Routledge (65-74).

Shamir, R. (2013). *Current Flow: The Electrification of Palestine*. Stanford: Stanford University Press.

Star, S. and A. Strauss (1999). Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work. *Computer Supported Cooperative Work* 8 (1-2): 9-30.

Strathern, M. (2018). Infrastructures in and of Ethnography. *Anuac* 7 (2):49-69.

Thylstrup, N. (2019). *The Politics of Mass Digitization*. Boston: MIT Press.

Van Dijck, J. (2009). Users Like You? Theorizing Agency in User-Generated Content. *Media, Culture & Society* 31 (1):41-58.

Wenger, A. and S.-C. Fischer (2021). Artificial Intelligence, Forward-Looking Governance and the Future of Security. *Swiss Political Science Review* 27(1): XXX-XXX.