Actor-Network Theory of Cyber-Security*

Thierry Balzacq† Myriam Dunn Cavelty‡

October 5, 2012

Abstract

This paper examines the import of Actor-Network Theory (ANT) in the field of cyber-security. Typically, cyber-security, which is computer-supported, is derivative of the "intermediaries" that actors put into circulation. The paper explores the politics and effects of one such intermediary: computer viruses. In fact, the paper argues, viruses are the fundamental "life forms" through which and by which actors define one another. What makes viruses analytically noteworthy is that they are not co-extensive with one single space (the network) as cyber-security studies often assume. Instead, viruses manifest themselves within different, overlapping topologies (regions, networks, fluids). In contrast to ANT, which claims that intermediaries remain spatially stable, the paper argues that intermediaries have an ambiguous ontology: they vary while they remain the same, from one location to another. Accordingly, cyber-security does not operate within an Euclidian space nor does it deal with ontological blocks. It is concerned with "intermediaries" that enacts their own spaces, depending upon the competence they are endowed with by actors. Thus, by focusing on different viral disruptions in the cyber-security discourse, the paper demonstrates how spaces produced by cyber-security are grounded upon specific, but changing/changeable claims of legitimacy, authority and power.

---

* Comments, welcome: thierry.balzacq@ed.ac.uk, dunn@sipo.gess.ethz.ch

† Honorary Professor at the School of Social and Political Science, Fellow, The Institute for Advanced Studies in the Humanities, The University of Edinburgh, 2 Hope Park Square, Edinburgh EH8 9NW.

‡ Lecturer and Head, Risk & Resilience Research Group, Centre for Security Studies, ETH Zurich (Swiss Federal Institute of Technology), Haldeneggsteig 4, IFW (B 49.2) 8092 Zurich / Switzerland.

1 INTRODUCTION

Since its beginnings, the concept of "network" has been a cornerstone of cyber-security.[1] The term network captures the imagination of cyber-security analysts in important part because the different technologies that constitute the texture of the cyber-space conjure up ideas such as interconnection, nexus, circuitry, but also structure and system.[2] On this view, cyber-security refers to a set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information.[3] This has the consequence that cyber-security depends essentially upon two complementary processes: secure the mobility of data, on the one hand, and ensure the stability of networks of relations that compose and sustain the cyber-space, on the other hand. The networked organization of the space enables targeted interventions of security actors. Ultimately, the network is controllable.

Contrary to previous understandings, an increasing number of scholars argue that there is not one, unique cyber-space. In this way, cyber-security occurs in different topologies, each marked with its own characteristics. For instance, Nick Bingham touts the illusion that "cyber-space as a singular exists at all."[4] Stephen Graham suggests that 'cyberspace…needs to be considered as fragmented, divided and contested multiplicity of heterogeneous infrastructures of actor-networks.'[5] Either way, however, scholars tend to assume that the different spaces thus enacted remain

---

1 Cf. John Arquilla and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica: RAND, 1996).

2 Cf. Steven Shaviro, *Connected, or What it Means to Live in the Network Society* (Minneapolis: University of Minnesota Press, 2003).

3 However, note that the term cyber-security is a fairly recent addition to the bundled of practices and concepts that reach back decades. Information security, information assurance, computer security, network security, and critical information infrastructure protection, (CIIP) are closely related concepts. Where they are all found in various policy documents, cyber-security has become the prevalent term more recently, trumping over critical information infrastructure protection, which previously held that position (see: Myriam Dunn Cavelty and Manuel Suter, 'The Art of CIIP Strategy: Taking Stock of Content and Processes', in *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, eds. Javier Lopez, Roberto Setola, Stephen D. Wolthusen (Berlin: Springer, 2012), 15-38.

4 Nick Bingham, 'Objections: From Technological Determinism Towards Geographies of Relations', *Environment and Planning D: Society and Space* 14, no. (1996): 32.

5 Stephen Graham, 'The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology", *Progress in Human Geography* 22, no. 2 (1998): 178.

"networks". In other words, what is called cyberspace is a 'skein of networks'.[6] The main task of cyber-security experts is therefore to account for how and the conditions under which cyber-threats sail through different networks, and develop strategies to counter them effectively.

In this paper, we argue that cyber-threats have distinctive spatial effects, which condition both different understandings of cyber-security and the kind of operations it commands or accommodates. To develop our argument, we draw on recent revisions of Actor-Network Theory (ANT), in particular John Law, Annemarie Mol, and Vicki Singleton.[7] These researchers suggest that objects come in various configurations, each associated with spatial processes that prompt or support a recombination of relationships. Specifically, objects can emerge as "volumes" thriving in a regional Euclidian space, as "networks of relations" configuring a network space, and as "flows" that continuously adapt their shape in order to generate a fluid space. The paper suggests that the study of cyber-security should emphasize the *objects* that circulate within the different spaces and impart them with specific cast. The reason is that, different objects have implications for the way we conceptualize cyber-security, the processes that bring actors together, and the type of interventions that are made possible. The paper is a theory-driven empirical analysis. As such, our study is extended by an examination of one of the most spoken about but surprisingly understudied cyber-threats, namely computer viruses. We find that viruses are appropriated as '*contagium vivo fluidum* – a contagius living fluid'.[8] But, 'fluid objects are beyond the network conditions of possibility.' Conceived in this way, we argue, cyber-threats tend to enact fluid spaces. This space does not necessarily abide by the same semiotic system (what cyber-security is) as regions and networks, nor does it have compatible pragmatic systems (how to practice cyber-security).

---

6 Bruno Latour, *We Have Never Been Modern* (London: Harvester Wheatsheaf, 1993), 120.

7 For excellent statements of this position, see John Law, 'Objects and Spaces', *Theory, Culture & Society* 19, no. 5-6 (2002): 91-105; Annemarie Mol and John Law, 'Regions, Networks and Fluids: Anaemia and Social Topology', *Social Studies of Science* 24 (1994): 641-71; John Law, 'Objects and Spaces'; John Law and Annemarie Mol, 'On Metrics and Fluids: Notes on Otherness', in *Organized Worlds: Explorations in technology, Organization and Modernity*, ed., Robert Chia (London: Routledge, 1998), 20-38; John Law and Vicky Singleton, 'Object Lessons', *Organization* 12, no. 2 (2005): 331-55.

8 Original emphases. Joost van Loon, 'A Contagious Living Fluid: Objectification and Assemblage in the History of Virology', *Theory, Culture & Society* 19, no. 5-6 (2002): 107.

The paper proceeds in three sections. Section I contextualizes the discussion on cyber-security. Section II examines the spatialities of cyber-security, laying out the basics of ANT. Section III delves deeper into the enactment of cyber-security through a focus on viral performances.

2 SITUATING CYBER-RESEARCH IN SECURITY STUDIES

Despite concerted efforts and increasing sums of money spent by state and business actors on various aspects of cyber-security over the years, cyberspace does not seem to become more secure: A plethora of technical and governmental reports in the last few years show an upsurge in quality and quantity of malware and related costs, linked to an increasingly professionalized criminal market taking advantage of the virtual realm. In addition, several highly publicized cyber-incidents (GhostNet, Stuxnet, Flame, Anonymous hacks, etc.) have solidified the impression that cyber-attacks are becoming more frequent, more organized and sophisticated, more costly, and altogether more dangerous. Consequently, cyber-fears have spread in two directions: upwards, from the expert level to executive decision-makers and horizontally, from being an issue mainly discussed in US strategic circles to the top of the threat list of more and more countries.[9]

With this 'spread', a specific in/security logic is being diffused, which was moulded in US military colleges, RAND and US government circles in the 1990s.[10] It consists of fears about the vulnerabilities of a 'sprawling, open country knitted together by transportation, power and communications systems designed for efficiency not security'[11] and the disembodied adversaries that are likely to take advantage of these vulnerabilities through the anonymity provided by information networks. [12] However,

---

9 In 2011/12 alone, the following countries have released cyber-security or cyber-defence strategies: France, Germany, India, the Netherlands, the United Kingdom, the United States, and Switzerland.

10 In neo-liberally inclined and democratic polities, variations in threat perceptions and proposed policy-solutions are variations of details, not substance. For a comparison of policies see cf. Elgin Brunner and Manuel Suter, *The International CIIP Handbook 2008/2009 - An Inventory of Protection Policies in 25 Countries and 6 International Organizations* (Zurich: Center for Security Studies, 2008).

11 Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States* (Arlington, VA: George Mason University Press, 2006), 51.

12 The US is the main arena and target of this literature, even though some American strategists have focused on China and Russia (but only in order to reflect on US strategy in this domain). See for example: Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice* (Ft

this logic is not only grounded in a fear of networked adversaries, but also seizes the opportunity to turn network vulnerabilities into a strategic advantage. In this discourse, information and networked information technologies are represented equally as a threat, as threatened, and as an opportunity.[13] The Persian Gulf War of 1991 was presented as the first of a new generation of conflicts, in which the ability to manipulate, degrade or even paralyse an opponent's communications systems was key.[14] Ever since, cyberspace has both discursively and practically been turned into an additional operational domain for military conflict like land, sea, air, and outer space.[15] The power of deconstructive features is recognized and acted upon, and (military and political) power is located (also) in the medium of code, symbols, signs, and information.[16] Military victory becomes conditional upon technological control over powerful automated networked information systems. The global network society is conceptualized as a battlespace of infinite proportions,[17] on which networked forms of organization have the upper hand over hierarchical forms, due to their flexibility and adaptability.[18] Enemies are represented by symbols and their actions unfold their effects through this space/place anywhere instantaneously. Threats or dangers are no longer perceived as coming exclusively from a certain direction – traditionally, the 'outside' – but are system/network inherent; the threat is a quasi-latent characteristic

---

Leavenworth, 2004); James C. Mulvenon and Richard H. Yang (eds.), *The People's Liberation Army in the Information Age* (Santa Monica: RAND, 1998); Mary C. FitzGerald, 'Russian Views on Electronic Signals and Information Warfare', *American Intelligence Journal* 15 (1994): 81–7; Timothy L. Thomas, 'Russian Views on Information-based Warfare', *Airpower Journal*, Special Edition (1996): 26–35.

13 Elgin Brunner and Myriam Dunn Cavelty, 'The Formation of In-Formation by the US Military: Articulation and Enactment of Infomanic Threat Imaginaries on the Immaterial Battlefield of Perception', *Cambridge Review of International Affairs* 22, no. 4 (2009): 625-642.

14 Prominent examples include: Alan D. Campen, *The First Information Warfare* (Fairfax: AFCEA International Press, 1992); John Arquilla and David F. Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy*,12, no. 2 (1993): 141–65; Alan D. Campen, Douglas Dearth, and Thomas Goodden (eds), *Cyberwar: Security, Strategy and Conflict in the* Information *Age* (Fairfax: AFCEA International Press, 1996); Martin Libicki, *Defending Cyberspace* (Washington: National Defense University, 1997); John Arquilla and David F. Ronfeldt (eds), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997).

15 Cf. William J. Lynn III., Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* Sept/Oct (2010): 97–108.

16 David J. Rothkopf, 'Cyberpolitik: The Changing Nature of Power in the Information Age', *Journal of International Affairs* 51, no. 2 (1998): 325-360.

17 Michael Dillon, Michael, 'Network Society, Network-Centric Warfare and the State of Emergency', *Theory, Culture, and Society* 19, no. 4 (2002): 75.

18 Cf. John Arquilla and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica: RAND, 1996).

of the system, which feeds a permanent sense of vulnerability and inevitability for disaster.

In terms of quantity, the bulk of cyber-security publications is of a policy-oriented or problem-solving nature and does not communicate with any IR or other theories.[19] The two main questions that are being tackled are 'who or what is the biggest danger for an increasingly networked nation/society/military/business environment' and 'how to best counter the new and evolving threat'. Apart from this body of literature, research with a focus on political/security questions related to cyber-issues is rare. While media and communication studies, sociology, or cultural studies have long discovered cyber-issues as a noteworthy topic, they usually do not focus on security aspects; International Relations and (critical) security studies on the other hand are surprisingly silent on all things cyber-related overall.[20]

There are a few exceptions: One body of research focuses on 'Postmodern War'[21], the discourse on technical-military interaction that focuses on the centrality of information as the 'new metaphysics of power' as outlined above.[22] However, this type of research is interested in the larger shift in war fighting practices rather than specifics and is only loosely relating to the practice of cyber-security. Another body of literature is produced by the 'Munk School', which has consistently focused on issues like (electronic) surveillance and censorship and is thus mainly concerned with the creation of more *in*security by (state) actors through cyber-means.[23] It has,

---

19 Johan Eriksson and Giampiero Giacomello, 'The Information Revolution, Security, and International Relations: (IR)Relevant Theory?', *International Political Science Review* 27, no. 3 (2006): 221–44. Some of the few (and recent) journal articles remain a-theoretical in the tradition of strategic studies narrowly understood (cf. the whole issue of Survival 53, no. 1).

20 One explanation is that many scholars are tempted to exclude technical threats from security (studies) on the grounds of little discursive resemblance to political-military threats. See: Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009), 19.

21 Chris Hables Gray, *Postmodern War – The New Politics of Conflict* (London: Routledge, 1997); James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Complex* (Boulder: Basic Books, 2001); Chris Hables Gray, *Peace, War, and Computers* (London: Routledge, 2005).

22 Michael Dillon and Julian Reid, 'Global Liberal Governance: Biopolitics, Security and War', *Millennium Journal of International Studies* 30, no. 1 (2001): 59.

23 Cf. Ronald Deibert *Parchment, Printing, and Hypermedia: Communication in World Order Transformation* (New York: Columbia University Press, 1997); Ronald Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium* 32, no. 3 (2003): 501–

however, not followed one particular theoretical pathway (if it uses theory at all) due to the interdisciplinary nature of its setup. The third exception, situated in the larger vicinity of critical security studies, is a small (and somewhat discontinuous) body of literature by scholars that have used frameworks derived from (or inspired by) Securitization Theory to see how different actors in politics have tried to argue the link between the cyber-dimension and national security.[24] These texts capture various elements of the evolution and 'securitization' (or rather non-securitization) of cyber-security.[25] They support observations made elsewhere that the process of securitization in a given socio-political community is not restricted to one setting and one type of audience only, but often involves several, overlapping and multiple ones,[26] or that there are different political functions of and strategies behind security utterances.[27]

However, critical engagements with cyber-security remain analytically 'thin', as their focus and explanatory range is restricted in multiple ways. First, these studies focus narrowly on politically salient speech acts by 'visible' political US figures that can be

---

530; Ronald J Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain, The Practice and Policy of Global Internet Filtering (Cambridge: MIT Press, 2008); Ronald Deibert and Rafal Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4, no. 1 (2010): 15–32.

24 Johan Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', *Journal of Contingencies and Crisis Management* 9, no. 4 (2001): 211–22; Ralf Bendrath, 'The American Cyber-Angst and the Real World – Any Link?', in *Bombs and Bandwidth: The Emerging Relationship between IT and Security*, ed. Robert Latham (New York: The New Press, 2003), 49–73; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008); Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53 (2009): 1155-1175; Sean Lawson, 'Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats,' *Journal of Information Technology & Politics* (forthcoming).

25 When not only focusing on threat representations – which are full of military analogies and 'multi-dimensional cyber disaster scenarios' (Hansen and Nissenbaum, Digital Disasters, 1164) – but on the actual countermeasures, the significant difference between the alarmist content of the threat representations and the selected 'normal' policies becomes obvious.

26 Thierry Balzacq, 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations* 11, no. 2 (2005), 171–201; Sarah Léonard and Christian Kaunert, 'Reconceptualizing the Audience in Securitization Theory', in *Securitization Theory: How Security Problems Emerge and Dissolve*, ed. Thierry Balzacq (London: Routledge, 2011), 57–76.

27 Juha A. Vuori, 'Illucutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders', *European Journal of International Relations* 14, no. 1 (2008): 65–99.

approved (or disproved) by general public. Such a focus reveals the constitutive effects the discursive practices of 'capable actors' have in (world) politics, but it is blind towards how these discursive practices are facilitated or thwarted by preceding and preparatory discursive and non-discursive practices of actors that are not as easily visible, also outside of governments.[28] Second, cyber-security is as a type of security that enfolds in and through cyberspace, so that the making and practice of cyber-security is at all times constrained and enabled by this environment and its technical logic. Cyber-(in)-security is therefore inseparable from the technical-material (referent) 'object' that it deals with: computers and computer networks. This factor is ignored by most of the literature. Third, due to their emphasis on official statements by 'the heads of states, governments, senior civil servants, high ranked military, heads of international institutions'[29], existing scholarship only grasps a limited expression of cyber-in-security (usually cyber-war) that is topmost on these people's minds.

Cyber-security, we contend, is both less and more. It is 'less' because it is not only and not often about situations of greatest urgency. It is a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. And it is far more, because multiple actors use different threat representations employing differing political, private, societal, and corporate notions of security to mobilise (or de-mobilise) different audiences. In fact, there are many layers of social interaction in several social spheres that characterize cyber-security. In today's increasingly cybered world, cyber-security is co-produced by every private computer user, by computer security specialists and IT support staff in the server rooms of this world, by programmers, by Chief Information Officers (CIOs) or Chief Executive Officers (CEOs) deciding on cyber-security investments, by IT-specialists working to secure government networks, by security consultants, by cyber-crime specialists, by cyber-forensics, by regulatory bodies and standardization organisations, and only *last* by politicians and other government officials that interpret digital events and (re-)act to them in the form of verbalized expectations and fears or ultimately, policies.

---

28 Jef Huysmans, 'What's in an act? On security speech acts and little security nothings', *Security Dialogue* 42, no. 4-5 (2011): 371.

29 Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (London: Routledge, 2006), 64.

In sum, what is missing from previous studies is a more close reading of the social practice of cyber-security and a better understanding of the material underpinnings of this discourse upon which this social practice unfolds. To understand more fully how cyber-security practices are changing and stabilizing claims of legitimacy, authority and power, an approach is needed that takes both these aspects (and their interrelationship) seriously. Actor Network Theory (ANT) promises to provide such a theoretical toolset. The relevant concepts and theoretical assumptions are shown in the next section.

3 ACTOR-SECURITY NETWORKS

The primary concern of ANT is with network-tracing processes.[30] It develops a "generalized ontological symmetry" whereby different kinds of entities (humans and non-humans) are involved in relational productive activities.[31] To catch the differences between entities, one needs not to look at their 'natural' or 'essential' features but, instead, at their semiotic configurations. For ANT, "*spaces are made with objects*."[32] Thus, the task of ANT is to account for the circulation of objects, the structures of relations they activate and the spatial im/possibilities they countenance. John Law sums up ANT argument on the relation between object and space in this way: "when a (network) object is enacted, so, too, a (network) world is being created with its own spatiality and its own versions of homeomorphism and rupture."[33]

In general, cyber-security analysts could find this view promising, arguing that the main vulnerability of cyber social order arises from the heterogeneous relations within and through which networks thrive. Understood this way, the aim of cyber-*security* is to secure the immutability and the mobility of the objects that make up the network. Put otherwise, cyber-security concentrates on what moves and how this movement

---

30 Bruno Latour, *The Pasteurization of France* (Cambridge: Harvard University Press, 1988), 171. A good discussion of the network trajectories is offered by John Law, 'Transitivities', *Society and Space* 18, no. 2 (2000): 133-148.

31 See Alex Preda, 'The Turns to Things: Argument for a Sociological Theory of Things', *The Sociological Quarterly* 40, no. 2 (1999) : 357 ; Bruno Latour, *We Have Never Been Modern* (Cambridge : Harvard University Press, 1993) ; Bruno Latour, 'Pragmatogonies : A Mythical Account of How Humans and Non-Humans Swap Properties', *American Behavioral Scientist* 37, no. 6 (1994) : 791-808 ; Doyle E. McCarthy 'Toward a Sociology of the Physical World : George Herbert Mead on Physical Objects', *Studies in Symbolic Interaction* 5, (1984) : 105-121.

32 Original emphasis. Law, 'Objects and Spaces', 96.

33 Ibid., 96-7.

commands different spaces, operating under different modalities. This is important because it is precisely spatial consciousness (or rather spatial anxiety, to paraphrase Foucault), which made the community of cyber-security analysts to translate the imagination of modern geography, with its Euclidian presuppositions, into the language of cyber-space.[34] Cyberspace has almost exclusively been represented as a place/space with a networked character. Grasping cyberspace as a place allows different notions of control and domination over the virtual domain. In its early days, the space-metaphor, suggested an unexplored land, freedom from legal and social constraints ('Western Frontier'), and opportunities in line with the cyber-libertarian-agenda that supports minimal Internet regulation/state involvement. Cyberspace was depicted by these 'pioneers' as a 'space' between the hardware components of computer networks, a place which is fundamentally different from reality, as 'the new home of Mind', 'a world that is both everywhere and nowhere, but it is not where our bodies live'[35] – but a place which fundamentally *is*.

On this view, cyber-security aims to safeguard the immutability of objects, despite the scale of the connections they perform. In turn, the intensity of a cyber-threat can be read in the severity of the disruptions/damages and is a function of the number of connections thus affected. In contrast to current accounts, however, this section argues that cyber-security does not unfold exclusively in a network-type of space.[36] If this were the case, cyber-security concerns would be easier to sort out and the policies to tackle them would perhaps be more effective, as the topology of a network, in part because of its reliance on "nodes" (i.e. points of the network through which objects *have to* transit), enables a centralized control to be deployed more or less straightforwardly. The problem is that cyber-threats are topologically complex. They often, or rather usually exist within different spaces, or co-emerge with different

34 The necessity to territorialize a milieu, as the precondition for the emergence of an assemblage (a form of actor-network), is developed in Gilles Deleuze and Félix Guattari. An assemblage "operate", they say, "in zones where milieus become decoded: they begin by extracting a territory from the milieus. Every assemblages is to discover what territoriality they envelop…. The Territory is more than the organism and the milieu, and the relation between the two, that is why the assemblage goes beyond mere 'behaviour'." Gilles Deleuze and Félix Guattari, *A Thousand Plateaux: Capitalism and Schizophrenia* (London: Athlone, 1988), 503-4.

35 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 1996, Electronic Frontier Foundation Website, available at <http://homes.eff.org/~barlow/Declaration-Final.html>

36 Jussi Parikka, 'Contagion and Repetition: On the Viral Logic of Network Culture', ephemera 7, no. 2 (2007): 287-308; Eugene Thacker, 'Networks, swarms, multitudes', *CTheory*, 05/18/2004 [http://www.ctheory.net/articles.aspx?id=422].

spatialities. Thus, in addition to networks, this section examines two other topographies of cyber-security, namely regions and fluids. Each spatiality activates a set of object im/possibilities, and vice versa. In short, "a fluid possibility, is network impossibility."[37]

Cyber-threats can only be read and tackled in the spaces they have built themselves, not in the one that is supposed to predate their enactment (i.e., networks). In other words, to understand cyber-security, it is necessary to complement the network and regional spaces that presently dominate the discussion, with a fluid approach to cyber-security that was thwarted by the previous two. The claim is not that neither networks nor regions matter; it is, instead, that cyber-security is not tied either logically or necessarily with these topologies. Our argument suggests that if cyber-security is so difficult to handle, as current governmental action suggests, this is due to the fluidity of its objects, not primarily to their networked or regional character. Cyber-security deals with flows; its space is fluid. Specifically, drawing from John Law and Annemarie Mol, we will show below that network-objects do not pose a particularly acute challenge to network-spaces; flows do.[38]

In the remainder of this section, we present the main concepts and theoretical tenets of actor-network theory. In so doing, we clarify the extent to which actor-networks

---

37 John Law, 'Objects, Spaces, Others', p. 9. Available at http://www.lancs.ac.uk/sociology/soc027jl.html (accessed on June 3, 2003). See also John Law, 'After ANT: Complexity, Naming and Topology', in *Actor Network Theory and After*, eds. John Law and John Hassard (Oxford: Blackwell, 1999), 15-25. The concern with different understandings of the dialectics among the spaces that a digital world render in/active is an important characteristic of researchers who use ANT for various purposes; see Nigel Thrift, 'New Urban Eras and Old Technological Fears: reconfiguring the Good Will of Electronical Things', *Urban Studies* 33, no. 8 (1996): 1463-93; Ralph Schroeder, 'Cyberculture, Cyborg Post-Modernism and the Sociology of Virtual reality Technologies', *Futures* 26, no. 5 (1994): 519-528; Mark J. Stefik, *Internet Dreams: Archetypes, Myths and Metaphors* (Cambridge: MIT Press, 1996); Steve Graham and Simon Marvin, *Telecommunications and the City: Electronic Spaces, Urban Places* (London: Routledge, 1996); Scott Kirsch, 'The Incredible Shrinking World? Technology and the Production of Space', *Environment and Planning D: Society and Space* 13, no. 5 (1995): 529-55; William J. Mitchell, *City of Bits: Places and the Infobahn* (Cambridge: MIT Press, 1996).

38 The fact that we rely on John Law and Annemarie Mol to build our argument aligns us with theorists of ANT whose fundamental concern is with the relationships among topography, epistemology and ontology. For excellent statements of this position, see Mol and Law, 'Regions, Networks and Fluids: Anaemia and Social Topology'; Law, 'Objects and Spaces'; Law and Mol, 'On Metrics and Fluids'; John Law and Kevin Hetherington, 'Materialities, Spatialities, Globalities', in *Knowledge, Space, Economy*, eds., John Bryson, Peter Daniels, Nick Henry, and Jane Pollard (London: Routledge, 2000), 34-49.

continuously enact their social spaces, emphasizing that the key to this spatial performance is the generation of an object, which sustains or disrupts a functional order.

3.1 Intermediaries

By situating the concept of network at the centre of its investigation, ANT parts way with classical geography in three significant respects. First, it substitutes the imagination of association for the classical Euclidian metrics mapped on position, proximity, and distance. In this view, places are the effects of distinctive relations among actants, not explanatory foundations.[39] Second, when classical geography tends to conceive spaces as a pure container for objects, ANT reconciles spaces and objects, arguing that spaces are performed by and through objects. On this view, then, the separation between objects and spaces is artificial. Finally, in contrast to classical geography, ANT does not treat the difference between 'digital' and 'physical' spaces as a matter of essence, but as the expression of their specific framing properties.[40]

The emergence of object relative to the enactment of space is therefore crucial to understanding topography's analytical importance for cyber-security. As different objects can enact various spaces, there is not one single cyberspace. Instead, as Stephen Graham argues, "there are multiple, heterogeneous networks, within which telecommunications and information technologies become closely enrolled with human actors, and with other technologies, into systems of sociotechnical relations across space."[41] However, the multiplicity of cyberspaces is not exclusively derivative of the sum of threats involved; nor it is function of the actants that are put into relations. These certainly contribute to the fragmented character of the cyberspace. Yet, the fact that there are several kinds of connections among actors of varied amalgams, does not necessarily end up into differentiated cyberspaces. An approximate (that is, imperfect) image is to say that cyberspace exists by virtue of what circulates within its meshes. For ANT, indeed, different objects create the

---

39 See Bruno Latour, 'A Relativist Account of Einstein Relativity', *Social Studies of Science* 18, no. 1 (1988): 3-44.

40 See Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (New York: W. W. Norton and Company, 1999). A eloquent account of the interaction among space, software and everyday life is offered by Rob Kitchin and Martin Dodge, *Code/Space: Software and Everyday Life* (Cambridge: MIT Press, 2011).

41 Stephen Graham, 'The End of Geography or the Explosion of Place?', 178.

possibility of spatial heterogeneity. Michel Callon calls these objects with spatial generative capacities, "intermediaries", that is, "*anything passing between actors which defines the relationship between them*."[42] It is the intermediaries that are the "real" concern of cyber-security. Intermediaries shape their networks in the sense that they are constitutive of its fabric. According to Callon, intermediaries are "defined by their roles, identities, and their program—which all depend on the relationship into which they enter."[43] The strength of the relationship is irrelevant. The role of intermediaries is generating and configuring interactions; in short, it is to compose spatial conditions and/or possibilities.

In this light, the definition of a cyber-threat is simultaneously the definition of its socio-technical context; that is, its space. The difficulty, however, is that a cyber-threats is not localizable in a clear sets of coordinates. It does not limit itself to replicating one space, but actually sets up alternative spaces. Importantly, Mol and Law insist, intermediaries perform "several kinds of spaces in which different 'operations' take place."[44]

This argument raises a quandary for ANT. In general, ANT contends that intermediaries maintain their composition regardless of the scale of the connections they hold together or bring into contact. Moreover, intermediaries are constituted by a more or less stable structure in a network of relations.[45] True, intermediaries that circulate and give cyberspace a specific texture can remain immutable throughout; however, this overlooks the many cases in which intermediaries mutate, alter their program, but keep their role, from one connection to another. In cyberspace, intermediaries often change, which means that stability is not the primary characteristic of the relationships generated by intermediaries. Thus, the aim of cyber-security is to deal with different kinds of intermediaries, including those that change their shape in order to release their agency and survive. These are "fluid" intermediaries, as opposed to "networks" and "regional" intermediaries.

---

42 Original emphases. Michel Callon, 'Techno-Economic Networks and Irreversibility', in *A Sociology of Monsters: Essays on Power, Technology and Domination*, ed., John Law (London: Routledge, 1991), 134.

43 Ibid., 139.

44 Mol and Law, 'Regions, Networks and Fluids', 643.

45 Law and Singleton, 'Object Lessons', 337.

3.2 Network Limits

This section argues that the fact that cyber-literature speaks of "networks" is not neutral, neither ontologically nor spatially. It indicates the type of objects it tends to be concerned with and the spatial conception it commands. Computer scientists seem to concur that it is inappropriate to claim that there exists one unique cyber-space: Any effort to map cyberspace (or the Internet) is usually incomplete and out of date the moment it appears.[46] It is constantly changing shape and form materially because new physical nodes and connections are made or disconnected. On a virtual level, new data and content is constantly created, altered, or deleted by millions of users. Functionally, new applications and new functionalities are changing and being changed by the behaviour of millions of users. Nonetheless, cyber-experts tend to derive spatial differentiations from actors' attributes and the relationships that bring these together. They conform, in this way, to a network approach to space. In other words, there are many overlapping networks, which sustain a variety of cyber-spaces. Basically, the difference is in form not in kind. In this section, we attempt to amend this view, arguing that cyber-spaces perform themselves differently, not only in forms but also in kinds. In the domain of cyber-security, three visions of spaces, in which riddle three manifestations of intermediaries stand out: regions, networks, and fluids. It is argued that cyber-security means different things within each of these spaces; each space has its own mode of ordering and calls for distinctive operations of power, authority and legitimacy. To increase the legibility of the argument, this section presents the regions' theoretical contours, while the practical inscriptions are discussed in the next section.

Regions. These are probably the most familiar, and straightforward spaces that IR scholars encounter. Regions connect and unite what is close and draw boundaries around elements that belong together. In a regional space, divisions between inside and outside are strict, places are exclusive, and overlaps between locations are not tolerated. Regional topography, we know, has shaped IR imagination for a long time, and in particular through the invention and institutionalization of borders and

46 R. Siamwalla, R. Sharma, and S. Keshav, 'Discovering Internet Topology', Technical report, Cornell University Computer Science Department, July 1998, http://www.cs.cornell.edu/skeshav/papers/discovery.pdf.

sovereignty.[47] Regions cluster objects together. Their primary aims if not their results is to suppress or minimize the differences among objects that reside inside and, correlatively, to play out the differences with what lies elsewhere. Those differences are meant to be solid.

Networks. At first sight, networks undermine most regions' basic assumptions, in part because networks establish relationships between elements that, in regions' terms, are distant on the map. Put more generally, the localization of objects does not determine their proximity and, as such, boundaries are not decisive in drawing out objects' identity. On closer inspection, however, regions follow from networks, and networks replicate regions' concerns with the ability of the object to preserve its integrity when it displaces itself from one location to another.[48] Conceived in this way, networks sustain what David Harvey calls "cogredient", that is, "the way in which multiple processes flow together to constitute a single constant, coherent, though multi-faceted time-space system."[49] The idea is that there is a relational isomorphism between regions and networks.[50]

A network space is generated by a network-object. Because this claim can easily be misinterpreted, it is worth noting that, for ANT, many objects, from texts to vessels through software, are 'networks'. In order to preserve their integrity, they depend on a stable structure of relations between their internal components and the external configuration of interactions they fold in. To move as a vessel from Amsterdam to Lagos (Euclidian space), the "relative syntactical positions of the vessel" (network-space) have to be held together, otherwise the network collapses.[51] On this view, the security of a network is very much about "*keeping everything in its place*."[52] In this context, objects are perceived to be threatening if they disrupt either the "cogredient" of the functional integrity of the network. The network-object loses its coherence, and the syntactical relations which held it rigid are henceforth subject to constant changes;

---

47 See R.B.J. Walker, *Inside/Outside: International Relations as Political Theory* (Cambridge: Cambridge University Press, 1992).

48 Mol and Law, 'Regions, Networks, Fluids', 649.

49 David Harvey, *Justice, Nature and the Geography of Difference* (Oxford: Blackwell, 1996), 260-1.

50 John Law, 'Actor Network Theory and Material Semiotics', unpublished manuscript, April 2007, 8.

51 Law, 'Objects and Spaces', 95.

52 Original emphases. Brian P. Bloomfield and Theo Vurdubakis, 'The Outer Limits: Monsters, Actor Networks and the Writing of Displacement', *Organization* 6, no. 4 (1999), 626.

in fact, everything becomes variable. This is the realm of fluid spaces and fluid objects, to which we now turn.

Fluids. Unlike networks, objects within a fluid space do not depend on one another, though they tend to coalesce because of the viscosity to the space. Networks tend to crumble if any of their constitutive parts is detached from the relational architecture that sustain them. By contrast, fluids are more resilient to the changing character of their objects. And, while objects composing a fluid space might be different, this difference is not the result of a given set of boundaries. In fact, networks and regions preserve their continuity by identifying crucial centres or points of vulnerability that must be defended against intrusions. On this view, security is fundamentally about protecting the "obligatory points of passage."[53]

There are important differences between networks and regions to be sure, but security is defined in both spaces as stability and immutable continuity. Fluids have a very singular shape, which has implications for the way security is understood therein. In fluid spaces, as Mol and Law put it: "there is no single standpoint to be defended in order to preserve continuity…. For since continuity has nothing to do with the integrity of territory in a fluid space, there are no fixed frontiers to be patrolled. Neither is there need for police action to safeguard the stability of elements and their linkages – for there is no network structure to be protected."[54] As they infiltrate other spaces, fluids absorb networks and regions, usually in part and rarely in total. Sometimes, networks and regions melt into fluid spaces. But this does not mean that fluids are the only spaces or objects available. But it does indicate the remarkable colonizing drive of fluids. However, even though its viscosity enables it to translate other objects into fluids, a fluid space reaches its limits when it cannot longer absorb other spaces or when it "encounters another immiscible liquid."[55] It is the relative viscosity of a fluid that determines both its strength and its weakness.

To summarize: nothing above suggests that we support a normative approach to the three spaces. This section was not concerned with the intrinsic value of any of the three spaces; it was, rather, focused on excavating their analytical leverage, in order to transfer it into the field of cyber-security. Whether called "real", "virtual", "digital",

53 Mol and Law, 'Regions, Networks, and Fluids', 661.

54 Ibid., 662.

55 Ibid., 664.

or “physical”, our argument has been that any world expresses a specific object/space articulation, which defines its complexion. Further, the different spaces are not mutually exclusive. And, while any space attempts to situate itself as the “other” of alternative spaces, it is in fact profoundly linked to the existence of these spaces. In this way, regions come across as a strategy to tame the variability of fluid objects; networks challenges the Euclidian spatiality of regions and sometimes melt into fluids. But, fluids possibilities are networks and regions impossibilities. Cyber-security doesn’t emerge only *as* or *in* a network. Instead, it is negotiated *within* and *among* the three spaces, each activating different types of operations.

4 VIRAL CYBER-(IN)-SECURITY PERFORMANCES

5 CONCLUSION