Cybersecurity, bureaucratic vitalism and European emergency

Simon, S.; de Goede, M.

DOI
10.1177/0263276414560415

Publication date
2015

Document Version
Final published version

Published in
Theory, Culture and Society

Special Issue: Governing Emergencies

Theory Culture & Society

Theory, Culture & Society
2015, Vol. 32(2) 79–106

DOI: 10.1177/0263276414560415
tcs.sagepub.com

SAGE

Cybersecurity, Bureaucratic Vitalism and European Emergency

Stephanie Simon and Marieke de Goede
University of Amsterdam

Abstract
Securing the internet has arguably become paradigmatic for modern security practice, not only because modern life is considered to be impossible or valueless if disconnected, but also because emergent cyber-relations and their complex interconnections are refashioning traditional security logics. This paper analyses European modes of governing geared toward securing vital, emergent cyber-systems in the face of the interconnected emergency. It develops the concept of 'bureaucratic vitalism' to get at the tension between the hierarchical organization and reductive knowledge frames of security apparatuses on the one hand, and the increasing desire for building 'resilient', dispersed, and flexible security assemblages on the other. The bureaucratic/vital juxtaposition seeks to capture the way in which cybersecurity governance takes emergent, complex systems as object and model without fully replicating this ideal in practice. Thus, we are concerned with the question of what happens when security apparatuses appropriate and translate vitalist concepts into practice. Our case renders visible the banal bureaucratic manoeuvres that seek to operate upon security emergencies by fostering connectivities, producing agencies, and staging exercises.

Keywords
complexity, emergency, cybersecurity, Europe, resilience

> In tomorrow's world, if the internet is not secured, nothing will be. (EU Commissioner Neelie Kroes, 2012)

Introduction

In a recent speech, Neelie Kroes, then Vice-President of the European Commission, echoes the widely held belief that the internet is the vital

Corresponding author: Stephanie Simon. Email: simon@uva.nl
Extra material: http://theoryculturesociety.org/

motor of contemporary life and that it may become the battlespace of the 'next big emergency' (e.g. North Atlantic Treaty Organization, 2010; World Economic Forum, 2011). Cyber-systems are cast as perhaps the most important of all infrastructures, not only because their breakdown is seen to pose potentially the gravest dangers – as when the control systems of power plants become corrupted – but also because modern life is considered to be impossible or valueless if disconnected. The complex interconnection of cyber-infrastructures forms a vast topological mesh where small events and disruptions can impact relations and elements near and far. Thus, securing 'cyberspace' has arguably become paradigmatic for modern security practice in the sense that 'disconnectedness defines dangers' (Barnett, quoted in Reid, 2006: 30). Cyber-systems are considered vital to life to such an extent that they *cannot* fail, they *must* absorb inevitable disruptions and emergencies.

This twin emphasis on the distributed and 'vital' cyber-infrastructure and the dangers of disconnectedness produce what in Europe have been called 'peculiar governance challenges' (European Commission, 2009b: 1). This paper analyses the particular and indeed peculiar modes of governing geared toward securing cyberspace in the face of potential interconnected emergencies. In particular, we focus on the dispersed practices, networks, and knowledges of European security bodies attempting to work upon and build what they call a resilient 'internet interconnection ecosystem'. The cyber-threat imaginary is broad and refers to topics as diverse as cyberwar, cybercrime, state and corporate cyberespionage, disruption of internet services, privacy violations, and the spread of 'dangerous ideas' online. The dire pronouncements of the interconnected emergency are not always couched in the apocalyptic language of digital inferno and disastrous cyberwar (e.g. Clarke and Knake, 2010). More often, they are uttered in unison with the projected promise of digital technologies to fulfil urgent questions of development, livelihood, and societal happiness (European Commission, 2010a). Cyber-systems are simultaneously inscribed with potential collapse and life-giving power. Cybersecurity imaginaries resonate with contemporary security efforts to target or operate within complex, emergent events and flows (Dillon, 2007), which are often described as realms of potential emergency *and* as essential to creative growth and vitality. The ambition to practise security in the realm of complex emergence often takes the idealised form of distributed interventions that might be able to integrate and evolve with the intrinsic 'grace' of systems themselves. This ideal is in opposition to strict hierarchical structures that are thought ill-equipped to bend to surprising and emergent events. The focus of this paper is precisely on this ambition and the ways in which actual practices often fall short and become productive in other ways.

The modes of governing geared toward securing vital societal circulations in the face of potential cyber-emergencies have received relatively little attention within existing literatures (but see Lakoff and Collier, 2010; DeNardis, 2012). On the one hand, literatures have analysed cyber-securitization and the geopolitics of information warfare (Barnard-Wills and Ashenden, 2012; Hansen and Nissenbaum, 2009; Wall, 2008). Cyberwarfare has been typified as 'cyclonic' because of its 'complexity, dynamism and dispersed character' (Deibert et al., 2012: 18; Deibert and Rohozinski, 2010). These authors have critically analysed efforts to bound, regulate or restrict online content (Deibert, 2003; Zittrain, 2009; Raley, 2009). On the other hand, literatures have analysed the importance and genealogies of resilience as a practice of governing complex systems and securing what Julian Reid (2006) calls 'logistical life'. According to Jeremy Walker and Melinda Cooper (2011: 144), 'the concept of resilience is becoming a pervasive idiom of global governance' and a 'theoretical reference point for the full spectrum of contemporary risk interventions' (also Lentzos and Rose, 2009; Aradau, 2010; Lundborg and Vaughan-Williams, 2011; Reid, 2012). However, there has been little engagement between these literatures to date. If, on the one hand, the literatures on the geopolitics of cyberwar have to grapple with the centrality of resilience – and not necessarily restriction – as a mode of governing systems security, the literatures on resilience and logistical life, on the other hand, have yet to address the ways in which these security practices play out in relation to the field of cybersecurity.

What is particularly interesting about the cyber-milieu as a security problem is the way in which its architecture as a topological mesh exemplifies the interdependent relations and interconnections of 'global complexities' (Urry, 2003). The 'machine space' of software and code stretches from 'traffic lights and lifts… to vehicle fleet maintenance systems… to child protection registers', as Thrift and French (2002: 320, 314) have noted, and increasingly these societal functions are connected online (also Dodge and Kitchin, 2011). The extent to which software code and information infrastructures are intertwined with everyday life, in fact, might be conceivable only through imagining its failures – in this sense, the Y2K millennium fears played an important role in animating the imagination of interconnected emergency (Thrift and French, 2002: 314–15). Perhaps even more than civic catastrophes and contingencies (Adey and Anderson, 2011; Lakoff, 2007), then, the cyber-emergency is inscribed with the potential to cascade transnationally and across private/public hierarchies in unexpected ways. It is perhaps precisely this transnational and relatively unregulated dimension which explains why the European Union (EU) is seizing upon the cyber-threat

imaginary as a key domain through which to foster its security competences (Barry and Walters, 2003).

We offer the concept of 'bureaucratic vitalism' to analyse the productive capacity of cybersecurity explicitly geared towards building 'resilient', dispersed, and flexible European security assemblages. The aim of these bureaucratic translations of the vital is to foster non-state, non-regulatory security practices that might mirror the very circulations and modulating relations that compose the cyber-infrastructure itself. We deliberately juxtapose 'bureaucracy', with its connotations of 'slow, lumbering structures', on the one hand (Kuus, 2011: 423), with 'vitalism', and its connotations of '*becoming*... movement... action' (Lash, 2006: 323), on the other. This juxtaposition seeks to capture the way in which European cybersecurity governance takes modulating complex systems as object and model, *without* fully replicating this ideal in practice.

With reference to the first term – 'bureaucracy' – the EU has set up two bureaucratic agencies that function as entry points for practising cybersecurity. ENISA was created in 2009 as a dedicated European agency on network and information security. It is housed on the Greek island of Crete and has built an agenda around the creation of network resilience and cyber-exercises. The European Cybercrime Centre (EC3) was set up in 2012 to combat cybercrime and is housed at the European police agency Europol in The Hague. Both agencies have emphasized the 'surprising' and unpredictable nature of the cyber-domain and its attendant threats (Oerting, 2013; ENISA, 2011b). While distinction between the roles, practices, and jurisdictions of these two agencies are at times unclear, their relative bureaucratic solidity means that they serve as nodal points and manifestations of security competences in the often nebulous realm of cybersecurity. In particular, ENISA's showpiece practice of conducting emergency exercises is the most visible manifestation of the *practice* of cybersecurity in Europe and beyond. These bureaucracies are by no means the only ones charged with cybersecurity, but they are important reference points within the field and, we argue, they offer visibility onto bureaucratic translations of the vital.

In reference to the second term, vitalism is deployed in three different but related senses in our analysis of the ways in which cybersecurity is unfolding in Europe (Lash, 2006; Foucault, 1994: 250–79). First, it concerns a power that has 'life' as its object – in other words, a power that is protective and productive of a particular valued way of 'European life' (cf. Amoore, 2008; Reid, 2006; Dillon and Lobo-Guerrero, 2008). As such, it is intimately connected to scenario-based, economic future visions for Europe. Second, it concerns a mode of power/knowledge that is not mechanistic but process-based. It accords meaning to systemic elements on the basis of their functions, their relations, their 'coexistence' and 'internal hierarchy'. It is attentive to the continuous and

co-dependent modifications of organic structures (Foucault, 1994: 265; Fraser et al., 2005). Acting upon this vital force respects the 'energy of movement [and] vitality of adaptation' (Foucault, 1994: 274–5), while seeking to 'manage the potentially unruly conduct of sociomaterial assemblages, aligning them with broader economic and governmental objectives' (Barry, 2010: 95). Third, we deploy the notion of vitalism in order to capture the way in which resilience as an ideal of governing aims to act with suppleness and to mirror the unpredictable threats that it sees itself to be addressing. As an ideal of governing, resilience in the face of the vital strives for 'continuous modulation or variation' (Barry, 2010: 93). What it produces in practice, however, are 'perilous and flawed translations' of resilience that largely remain locked into prior registers of linearity and un/predictability (Abrahamsson, 2012: 316). Bureaucratic vitalism, in this sense, produces an everyday bureaucratic orientation to events and emergency that, we argue, deploys an impoverished sense of contingency.

Our analysis builds upon Michael Dillon's refashioning of Foucauldian biopolitics for a 21st century characterized by molecularization and digitalization, wherein 'it is neither geopolitics nor biopolitics alone but the toxic combination of the two that now drives western security practices' (2007: 9). Dillon contends that 'life' in contemporary biopolitics is distinct from territorial constructions of sovereign power or the population construction and 'species-being' of disciplinary power. Rather, life is ontologically understood as radically and fundamentally contingent. Through a liberal governmental lens, life and species-being are approached as emergent, complex, and non-linear rather than being ordered or disciplined statistically and juridically. Emergence, the processual becoming of life, things, and relations, is the ground upon which security is practised and the realm in which societal emergency is imagined. 'To be precise', Dillon and Reid write, 'the emergency of global liberal governance is a continuous state of emergence rather than a continuous state of exception' (2000: 136).

However, Dillon and Reid's framework (2009) may understand the 'liberal way of war' as rather too closed, capable, and fully realized, as has also been argued by Lundborg and Vaughan-Williams (2011). While the ontology of contingency and emergence pervades foundational understandings of contemporary security, this does not mean that it is seamlessly replicated in practice. Thus, we are concerned with the question of *what happens when* governing bureaucracies appropriate and translate complex vitality. The 'specificity of the case' of internet security (Barry, 2010: 96), in our reading, is that it renders visible the banal bureaucratic manoeuvres that seek to operate upon security emergency by fostering connectivities, producing agencies, and staging exercises. The governmental embrace of the surprising internet and its inevitable shocks and excesses are routinized into particular governance effects that desire,

but can never fully realize, a self-organizing, emergent governance process that can meet and metabolize emergency events.

The Emergent Cyber-Milieu

Cybersecurity is entwined with the 'terrain' of cyberspace, which practitioners conceptualize as a complex, generative realm of emergent relations that are both material and immaterial. In this sense, apparatuses of cybersecurity aiming for vital dynamism are only thinkable in relation to an intrinsic cyber-spatiality, relationality, and virtual and material essence. We conceptualize the 'terrain' of cybersecurity in a Foucauldian sense as part of the *milieu* through which life is lived and the field of intervention at which apparatuses of security are directed. In his lectures on apparatuses of security, in distinction to but not separate from sovereign and disciplinary techniques, Foucault introduces the notion of political techniques concerned with the 'natural' elements of a lively milieu. Apparatuses of security are concerned with 'a multiplicity of individuals who... fundamentally and essentially only exist biologically bound to the materiality within which they live' (2007: 21). Foucault describes this conception of security and its allied spatiality of emergent environments as 'the entry of a "nature" into the field of techniques of power' (2007: 75). Whereas we might crudely ascribe a spatiality of territory to a sovereign *dispositif*, and enclosed spaces such as prisons and barracks to a disciplinary one, the milieu in a security *dispositif* is a space of emergent circulation through which life is lived and within which the intensive 'nature' of the population emerges. Rather than prohibitive sovereign or disciplinary mechanisms, which 'say no', a security *dispositif* wishes 'to say yes to... desire' (2007: 73). The distributed effects of apparatuses of security embrace 'the naturalness of the population' and its desire, inasmuch as they are the population's 'mainspring of action' (2007: 72). Thus, security interventions or points of entry through the milieu are, ideally, not primarily guided by notions of 'normation' or nullification but by the 'progressive self-cancellation of phenomena by the phenomena themselves' (2007: 66).

The internet is the milieu in which the valued life is imagined to be lived, or to which contemporary life is critically connected. Importantly, the milieu is not 'cyberspace'. Thinking about cybersecurity through the milieu allows us to get at the 'problematics of cyberspace' as an ongoing production and intertwining of material and immaterial relations and forces rather than an object or end-product (Crampton, 2003: 12; see also Cohen, 2007). For critical scholars, framing the cyber as milieu offers an alternative to the reification of 'cyberspace' as the 'fourth terrain' of warfare in mainstream strategy literatures (Betz and Stevens, 2013). The complex intertwining of the physical and the virtual is a

crucial component of cybersecurity, which is as much about the promises of the connected, online life as it is about protecting the integrity of fibre-optic cables. The milieu is both 'a materiality within which we live' and that to which we are 'biologically bound' (Foucault, 2007: 21).

There are, however, important differences between Foucault's conception of apparatuses of security in an 18th century, largely French context and a 21st century cyber-milieu. In the former context, while the naturalness of the population was thought to be complex, circulatory, and aleatory, it was also thought to be accessible and steerable through predictive and calculative techniques. Foucault calls this notion 'the penetrable naturalness of the population' (2007: 73). In contrast, contemporary apparatuses of security are more often oriented toward the incalculable and the unpredictable. Just as the new 'problem of the town' emboldened 'new mechanisms of power' like actuarial techniques, the security problematic of indeterminate milieus – such as the cyber-milieu – revolve around a *paucity of knowledge* and (ideally) techniques that might *potentially* be able to emerge in moments of uncertainty.

A part of the distinction to be made in pushing calculative interventions in a 'natural' milieu into the 'vital' digital realm involves acknowledging the embrace of complexity thinking in scientific thought, particularly in the biological and ecological sciences.[1] The term 'milieu' is rooted in scientific thought – as Foucault notes – where it has historically served as an important nodal point in debates about the causal relations between organisms and environments (Canguilhem, 2009). Monica Greco's work is instructive in drawing this link between the vital milieu and uncertainty in complexity thinking. Drawing on Stengers, Greco writes that the theme of complexity is important to vitalist thought because it 'intervenes to mark a leap in the order of possible knowledge, and therefore a difference in the quality of our ignorance' (2005: 22). This qualitative difference in possible knowledge is drawn out through Stenger's distinction between complexity and complication in a 'scientific view of the world'. Greco writes: 'A phenomenon is *complicated* when the task of predicting its behaviour presents a difficulty due to incomplete information, or to insufficient precision in the formulation of questions, but when in principle it is possible to explain and understand it by *extending* a simple, fundamental model' (2005: 23, emphasis in original). By contrast, Stengers identifies that the 'difficulty' of *complex* situations 'may not be due to a lack of knowledge, an incomplete formulation of a problem, or the enormous complication of the phenomenon, but may reside in *intrinsic reasons* that no foreseeable progress could gainsay' (Stengers, 1997: 8, emphasis added). Thus the intrinsic spatiality and relationality of the complex milieu stands in distinction to calculative techniques that attempt to know and maximize the natural

elements and desires of the population, and this notion of the *intrinsic* is precisely what cybersecurity ambitions identify as a point of entry.

While this is not the place for a comprehensive history of the internet nor a detailed discussion of its functioning and architecture, there are several crucial 'intrinsic' elements of the cyber-milieu that need to be drawn out in order to understand knowledge frames and tactics for anticipating and managing cyber-emergency, in particular the traits of redundancy, openness, and flexibility. First, data paths through cyber-networks are multiple, emergent and, to some extent, unpredictable. Early technological developments in data networking have their roots in defence and security research and development in the US Department of Defense Advanced Research Projects Agency (ARPA) where ARPANET was created, which would become the technological core of what eventually became the internet. Parts of ARPANET were the result of work in the 1960s to develop new command and control communication systems that could survive attacks in the Cold War context – the development of 'survivable communications' was rooted in the imagination of severely disabled communication systems in the event of a nuclear attack (Baran, 1964; see also Galison, 2001).[2] At this time, communications systems were highly centralized and dependent upon a small number of operators serving as switching nodes, directing traffic between points. These systems were quite vulnerable as damage to one node could disable an entire system. Packet switching was the key technological innovation leading to the development of 'distributed communications' rather than highly centralized systems. Packet switching, which remains a crucial element of internet functionality, involves breaking up data transmissions into 'packets' that are routed through networks independently of one another and reassembled to form the original message at their destination. This system involves switching nodes that themselves make decisions about how to route packets based on network traffic and other conditions. In effect, this means that there are multiple paths between two points and that these paths cannot be precisely known or controlled before they set out.

Decentralization and the unpredictability of multiple, potential pathways were key to the development of the ARPANET as a communication technology of security, but the development of the internet is not fundamentally a military or security story. The second trait of cyber openness and flexibility concerns the continual modulation, merging, and layering by users that extend far beyond network architects and original purposes. ARPANET was primarily used and developed by computer scientists, *not* the military, who were dispersed in academic institutions and tied to sites with supercomputers and who desired dispersed data-sharing and computer time-sharing. As data networks like ARPANET in the US and Cyclades in France became more common, networked applications and programming, were increasingly developed

and modified by users and guided by an ethos of trust, sharing and building connections. The introduction of email and the creation of the World Wide Web at the CERN labs in Geneva are examples of this user-driven ethos. The open structure of the internet is one of the legacies of this user-driven, dispersed, and collaborative development. The internet is not *a* network but a complex of interconnected networks and layers that are relatively unaware of one another, which made it possible for diverse networks and actors to connect and *inter*operate. This has remained incredibly relevant as the vast majority of cyber infrastructures are now privately owned. Since its commercialization in the mid-1990s, internet functionality has become bound to a web of private actors and interests. This assemblage of private cyber ownership is so well entrenched that the romanticized traits of private sector speed, flexibility, and technological innovation are now considered intrinsic elements of cyber functionality and health – to be fostered and respected by security practitioners – even as it adds another web of complex, obscuring inter-relations to the cybersecurity endeavour.

Further, despite the existence of certain groups such as ICANN, the Internet Corporation for Assigned Names and Numbers, which assigns globally interoperable identifiers for domain names and IP addresses, the internet has no centralized governance point. 'Protocol politics' (DeNardis, 2009) are deeply entrenched in the international technical and interoperability standards of the internet, but these are not best approached from institutional or sovereign perspectives. Rather, 'most of the real-world governance of the Internet is decentralized and emergent; it comes from the interactions of tens of thousands of network operators and service providers – and sometimes users themselves' (Mueller, 2010: 9). The relationship toward 'governance' in a digital realm, then, is not generally oriented toward sovereign, disciplinary or regulatory functions, but rather toward assemblages of dispersed actors that operate upon and within a relatively surprising cyber-milieu.

Intrinsic elements of the internet – the way it works, what it is, and how it came to be – are rooted in what Janet Abbate calls its 'protean nature' (2000). 'The constant in the history of the Internet', she writes, 'is surprise' (2000: 218), which is a result of this layered, interoperable, dispersed, user-driven and relatively unregulated design. This brief sketch of 'intrinsic' complexity is itself a reduction of cyber generation and dynamism, which has also been thoroughly documented in cybersecurity documents as well as in academic literatures (e.g. Mackenzie, 2005; Zittrain, 2009). In its contemporary manifestation, the internet is considered highly robust and secure because of these qualities of redundancy and flexibility. However, these same qualities are also cast as security threats; the internet is too dispersed, too complex, too lively, too integrated with daily life to really even get a picture of what it *is*, let alone to

be able to engage in consistently territorialized or disciplinary security practices upon it.[3]

The emergent, distributed design of the internet is said to make it a 'robust infrastructure' well prepared to withstand disruptions. Overwhelmingly, this is the conceptualization that shapes the cybersecurity landscape, even as the recognition of an intrinsically distributed, emergent internet makes it very difficult to imagine and *know*. EU cybersecurity agency ENISA describes this 'partial view' of the internet:

> Modelling the interconnection system is hard because we only have partial views of it and because it has a number of layers, each with its own properties and interacting with other layers. . . . *Resilience depends on the diversity of interconnections*, which in turn depends on physical diversity – which can be an illusion, and is often unknown. (ENISA, 2011b: 8)

Thus, the conceptual terrain of cybersecurity is set out and framed by a recognition of ignorance and the valorization of analytics geared toward the complex, which 'can lead to the conclusion that we do not know what a being is capable of' (Stengers, 1997: 6). This conceptual frame is thought to be distinct from that of a reductive frame that might instead say, 'if we had more knowledge, more methods of calculation, more facts, we could. . .' (1997: 6). This distinction marks out the distinction between apparatuses of security directed at a 'vital' milieu rather than a population believed to be more or less calculable.

Points of Entry in the Complex Emergency

The dispersed and complex nature of the cyber-milieu fuels what can be called a paradigmatic crisis imagination of transboundary, virulent and unpredictable escalation. More precisely, the premediation of cyber-emergency revolves around a notion of *cascading failure*. Infrastructural 'damage or interruption' has the potential to 'ripple across. . . technical and societal systems' and may have a 'force multiplier effect' (Dunn, 2005: 259). As such, 'even a relatively small attack [could] achieve a much greater impact', according to experts (p. 259; see also Grubesic and Murray, 2006; Little, 2002; Perrow, 1999). An EU Commission document gives some examples of possible 'widespread cascade effects' rippling through failing infrastructures:

> an attack on electrical utilities where electricity distribution was disrupted; sewage treatment plants and waterworks could also fail, as the turbines and other electrical apparatuses in these facilities might shut down.

Or, alternatively:

> [A] conventional bombing attack on a building [could be] combined with a temporary denial of electrical or telephone service. The resulting degradation of emergency response, until back-up electrical or communication systems can be brought into place and used, could increase the number of casualties and public panic. (European Commission, 2004: 3)

In this manner, so-called low-probability events are inscribed with the potential to have high and unexpected or unpredictable impacts on societal functioning and distant localities (ENISA, 2011b: 10; also Aradau and van Munster, 2011; Anderson, 2010).

Current emergency thinking focuses on transboundary crises that 'may escalate rapidly and morph along the way' and that transcend not just geographical and jurisdictional boundaries but that spill across functional systems, thus being confronted 'with different logics and operating imperatives' (Ansell et al., 2010: 195–6). The cascading effect is activated through information technology that underpins the many interconnected systems relied upon in everyday life, including telecommunications, electric power, water treatment facilities, emergency response systems, traffic signals and multi-sited industrial control systems (European Commission, 2004: 4). There are many ways in which 'failures can interact', as failures within high-risk systems display 'interactive complexity' (Perrow, 1999: 4). As one interviewee from the Dutch national cybersecurity centre explains, a cyber-crisis is very different in nature from a 'classical crisis'. If crises would normally be expected to start locally, spread slowly, and be managed – more or less – hierarchically, the cyber-crisis departs from this model through its rapid, interconnected, cascading failure and upsetting of neatly imagined hierarchies and response strategies. In an ICT crisis, 'there is no mayor', this interviewee states, 'no one owns the internet'.[4] The transboundary, unpredictable, cascading emergency produces unclear points of entry for responders dispersed across jurisdictional bounds, operating at the limits of knowledge.

In the face of the cascading crisis, cybersecurity directs itself at a milieu considered unmappable in its entirety and unknowable in its essence. Knowing and securing vital systems revolves around addressing, as Foucault (1994: 273) puts it, 'the enigma of a force inaccessible in its essence, apprehendable only in the efforts it makes here and there to manifest and maintain itself'. This includes physical infrastructures and network nodal points, but also 'the *services*' they deliver, as well as 'the physical and electronic (information) *flows*, their *role* and *function* for society, and... the *core values* that are delivered by the infrastructures' (Dunn, 2005: 263, emphases in original). An influential report prepared

for the European Commission by Bell Labs produces an 'eight ingredient framework' that lists potential points of entry for governing the modulating cyber-domain, including hardware, software, networks, payload ('information transported') and policy. The authors take comfort in the discrete listing of ingredients and supposedly finite 'intrinsic vulnerabilities' (ARECI, 2007: 13). But the list also signals to the incalculable points at which and ways in which failure could happen and, presumably, the points of entry for cybersecurity practice, including things (fuel, fuses, electronic circuit packs, transcontinental cables, semiconductor chips, internet exchange points), human relations (regulations, protocols, training, ethics, human-machine interfaces), and complex relational sites ('trenches where cables are buried', 'cell towers exposed to inclement weather') (2007: 28–9).

The lively materialities and 'leaky plumbing' (Roberts et al., 2012; Lundborg and Vaughan-Williams, 2011; Bennett, 2009) of infrastructures and their relations are not just complicated – they are complex. More information, knowledge, or general models cannot overcome this complexity, which is generally acknowledged amongst cybersecurity practitioners, even as describing and identifying has been one of the more clear requests from policy-makers. To date, one of the more concrete acts in European cybersecurity was the call to simply *identify* and enumerate critical European infrastructures (Council of EU, 2008). Much like ARECI's list of the eight information infrastructure 'ingredients' of the internet, recognizing and mapping critical infrastructures is exceedingly difficult because they are spread across an overwhelming array of blurred political and economic borders and the relations and dependencies between them are often complex and opaque. Techniques of identification are further obscured by the difficulty of defining what exactly is 'critical', as criticality is rooted in elusive promises of the modern life worth living in a 'knowledge-based economy' and an 'information society'.

Cybersecurity bureaucrats, then, face 'an eventful world' upon which attempts are made to 'pre-empt and redirect incipient events' composed of 'vibrant matter' and lively flows and interdependencies (Braun, 2011: 391). Rather than precise targets or locales, what these efforts wish to target are *the nodes, relations, and connections* between many different vital systems that are often unknown, privately owned, generative, and complexly interwoven. However intense and explicit this wish to embrace a lively, circulatory milieu, though, it would be a mistake to claim that the cyber-milieu is a lawless, open site without checks or controls. The claim that the internet is too open, too complex to govern, serves to obscure the emergent ways in which it *is* governed that bypass or ignore traditional political protocols.

In a recent event where she spoke about the trans-Atlantic cybersecurity relationship, the Deputy Secretary of Homeland Security,

Jane Holl Lute (2012), called this the 'great debate' in cybersecurity where the role of government is 'unclear' and 'polarizing'. She describes the poles as those who think there is no role for government in the open, user and market-driven cyber-realm and those who think there is a clear security role to be played in this emerging 'warzone'. In one sense her response of 'meeting in the middle' and 'balancing freedom, openness, and access . . . with security' is standard fare, but she goes on to state that the role for government in this middle ground is to figure out how to 'build that openness and that access in a way that also ensures resilience'. So, while we can point to moments in which cybersecurity officials explicitly wish to 'strengthen the hand of law enforcement', the guiding logic is not necessarily prohibition but openness and resilience in 'building a cyber-ecosystem' (2012). The (ideal) point of entry for security modalities oriented toward the environmental or intrinsic is not exactly, as Anderson notes, to enact 'milieu control' or to create an 'unliveable milieu' (Anderson, citing Sloterdijk and Lemov, 2011: 231) but to maximize or optimize 'natural' elements and their intrinsic 'grace'.

Lute's remarks pose resilience as a mode of governmental action, of governmental 'building', or active intervention, that might exist alongside the properties of cyber-emergence and self-fixing. In this way, 'resilience' does the discursive work of closing the yawning gap where security interventions meet a vital milieu, where it wishes to 'say yes to desire', and contemplates how they might initiate an embrace (Lentzos and Rose, 2009; Walker and Cooper, 2011). Like Lute, Andrea Servida from the Commission considers information infrastructures as 'the nervous system of the Information Society' and suggests that policy needs to be oriented toward cross-border and multi-partner complexity to 'tackle cyber attacks and disruptions from an ecosystem perspective' and to encourage a 'resilience culture' (Servida, 2009). EU network and information security practitioners similarly use ecosystem metaphors to imagine the complex relations and materialities of the internet. For ENISA, the 'Internet interconnection ecosystem is complex and has many interdependent layers. This system of connections between networks occupies a space between and beyond those networks and its operation is governed by their collective self-interest' (2011b: 4). According to the European Forum for Member States, the internet 'is not a private garden, but rather a complex ecosystem in which every participant must work together to ensure that their shared interests are fulfilled' (EFMS).

Resilient security practices do not aim to operate through suppression or prediction through risk calculus, but by attempting to embrace the surprising, eventful, and turbulent. In their genealogy of resilience, Walker and Cooper (2011) draw out two key elements of resilience governing that seem to have been fully embraced in the European cybersecurity agenda. First, it acknowledges and acts on the 'limits to predictive knowledge' and 'insists on the prevalence of the unexpected' (2011: 147).

Second, it sheds the notion of system equilibrium that was long dominant in the physical as well as economic sciences, in favour of an understanding that complex systems may be fundamentally mutated through shocks or crisis, while nevertheless preserving their vital functions. 'A complex notion of resilience', in the words of Walker and Cooper (2011: 146), seeks to 'account for the ability of an ecosystem to remain cohesive even while undergoing extreme perturbations'. One European bureaucrat articulates the resilience approach in explicit opposition to *avoidance* of incidents. Like floods or fires, internet attacks and information infrastructure breakdowns are considered to be to some extent inevitable. In the words of this practitioner: 'resilience doesn't mean avoidance . . . [what] counts [is that] you are able to recover soon . . .. So resilience in that sense is . . . related to fast recovery and fast response, rather than avoidance'.[5] When this ecosystem resilience logic is mobilized in the cybersecurity field, the *ideal* for governance practices is that actors could spontaneously behave in ways that flexibly complement the foregoing robustness of cyber-emergence. The ideal for cybersecurity points of entry is to encourage the potential to modulate and stretch *within* the emergence of cyber-relations in ways that do not bend beyond their 'natural' ecosystemic states. In his discussion of the 'complexities of the global', Urry (2003: 237) writes: 'Such complex social interactions have been likened to walking through a maze whose walls rearrange themselves as one walks. New steps then have to be taken in order to adjust to the walls of the maze that adapt to one's movement through the maze.'

By introducing the phrase 'bureaucratic vitalism' we mean to emphasize that this is an ambition more than a reality. Cybersecurity discourses may emphasize vitality and emergent flexibility, but, in practice, security techniques cannot necessarily and gracefully coevolve with incipient events and intrinsic complexity. In his discussion of the *politics* of contingency and vitality, Bruce Braun writes, 'demonstrating contingency can never be the goal in and of itself; it is rather just the beginning' (2011: 391). The politics of contingency does not end with the recognition that the world is 'overfull with potential'; what matters is that 'incipient events are *determined to be determined*, that is, they are always coming *to* a particular determination' (p. 391; emphasis in original). One thing that cybersecurity reveals is the bureaucratic translations of the vital *in practice*. The conceptual frame of acknowledging ignorance in the face of complex emergence is not something that can be seamlessly integrated into apparatuses of security that presume the necessity of intervening and shaping. This conceptual and discursive frame obscures the ways in which cybersecurity actively shapes how things come to be determined, without having to take responsibility for influencing things in some directions rather than others.

Bureaucratic Vitalism

We have argued that the way in which cybersecurity imagines its object of governance can be called 'vitalist' in the sense that it is attendant to the intrinsic complexity and lively nature of cyber-emergence. The milieu to be secured is thought of as an ecosystem and is inscribed with a dynamic essence that resists complete knowledge or mapping. At the same time, cybersecurity seeks to mirror or model itself on the vitalism of its threat object, and attempts to create 'resilience' or flexible security practices that could potentially bend and flex within the modulating cyber-milieu rather than produce interventions that would leave the internet more brittle, rigid or breakable.

Although vitalism itself is a concept in flux – a 'moving target' – it generally refers to a history of anti-mechanistic biological thinking that inscribes living matter with a measure of dynamism and mutability, rendering it resistant to capture through chemical or mechanistic processes (Normandin and Wolfe, 2013). In this sense, vitalism understands life in direct 'opposition to *mechanism*' and is attentive to processes of '*becoming* over *being*, of movement over stasis, of action over structure' (Lash, 2006: 323, emphases in original). As Lash (2006: 323–4) describes it, 'the primary distinction between mechanism and vitalism may be in terms of vitalism's s*elf-organization*. In mechanistic thought, causation is external: the paths or movement or configuration of beings is determined. In vitalism, causation is largely self-causation. And beings are largely indeterminate.' Greco similarly emphasizes vitalism's distinction from mechanism. As we have discussed, for Greco (2005: 18) what is perhaps most important about vitalism is that its respect for the excess of life recognizes the limits of modern science and offers a 'sort of label affixed to our ignorance'.

However, the appropriations of notions of vitalism and resilience by European bureaucracies tasked with cybersecurity do not produce a fully felicitous mirroring of vitalist emergence or dynamism. We should be careful not to overstate the measure to which security governing succeeds in becoming vital and in developing an ethos that respects ignorance. Instead, cybersecurity involves translations and appropriations of some elements of vitalist thought while discarding others. We seek to understand more precisely what happens in these translations, when governing bureaucracies appropriate the languages and logics of vitalism and resilience. Which elements of vitalist thinking are appropriated and incorporated into governing logics? Which elements are discarded or ignored? And if it is not fully rendered, what effects are produced from a security apparatus targeting and hoping to mimic complex emergence?

One important element of the cybersecurity bureaucracies' vitalist translation is a valuation of action over structure. Following Lash, we may say that the governing template of 'movement over stasis' and

'action over structure' is appropriated by cybersecurity agendas with specific effects. On the whole, cybersecurity is wary of rigid juridical frameworks and the fostering of supranational competences. ENISA (2011b: 5, 25) explicitly differentiates its approach from regulation, rejecting the notion that internet regulation should be a 'matter of National Security' and emphasizing that 'any policy should... proceed with caution'. ENISA (2011b: 25) asserts: 'Regulating a new technology is hard; an initiative designed to improve today's system may be irrelevant to tomorrow's, or, worse, stifle competition and innovation.' In other words, there is an acute awareness that technological innovation and market potential should not be stifled through what Foucault calls the 'juridical-disciplinary system' (2007: 37).

There is a valuation of the self-organizational capacity of cyber-innovation that is not to be restricted or tampered with through rigid measures or supranational directives. For example, notions of flexibility and openness in cyber-governance played an important part in discussions surrounding the 2010 adoption of the EU Framework Decision on Attacks against Information Systems. The language in this directive was kept 'as technologically neutral as possible', because, as one Council representative explained, 'it is no point creating legal instruments that will lose force because of technological development'.[6] At the same time, however, such 'technically neutral' and pertinently vague language creates an expansive field of potential security intervention in which the distinction between hacktivist practices and intentionally fraudulent operations has become difficult to draw.[7] The pace of technological innovation and the 'unpredictability of potential crises' are invoked in these debates to foster expansive security domains, 'flexible strategies' and modes of rapid response (European Commission, 2009a: 6).

While wary of rigid institutional templates, cybersecurity agendas are not passive in the face of commercial agendas, nor do they display a neat equation with neoliberalism – understood either as a particular orientation to market practice and commercial logic, or as the production of particular subjectivities (Larner, 2006). Action is routed through a plurality of action plans, workshops, initiatives and reports that are produced through European agencies, cybercrime centres and research institutes. It seeks a decentred distribution of security practice through the establishment of agencies, platforms, dialogues and so-called Computer Emergency Response Teams (CERTs), with the goal of developing a '*flexible European-wide governance framework*' (European Commission, 2010b: 5). In Foucault's terms (2007: 20), this may be understood as a 'multivalent and transformable framework' within which 'a series of events or possible elements ... will have to be regulated'.

This multivalent and mutable framework takes concrete shape in the European cybersecurity agenda through the formation and

empowerment of Agencies (ENISA and Europol), rather than the creation of supranational competences or spaces. According to resilience thinkers, transboundary crises 'cannot be managed or even coordinated in a top-down fashion from some central office', but require a 'self-organizing response system' (Ansell et al., 2010: 203). These authors hold up the European Union's informal coordinating mechanisms and agency-building as an example of such self-organizing systems that build 'administrative resilience' through 'intricate, scaled-up, coordination mechanisms' (p. 203). The 'agentification' of Europe as a form of governing that values action over structure, and informal coordination over the creation of supranational space, fits into a durable history of Europe as a 'technological arrangement' as opposed to a strictly political one (Barry, 2001: 20). These efforts are scarcely recognizable in terms of traditional security politics, yet they have important political ramifications. Specialist agencies are populated with expert but unelected technocrats, and questions are raised about the transparency and accountability of these new incarnations of Europe's historically important technocracy (Den Boer et al., 2008). ENISA and Europol largely perceive and present themselves as a-political points of interconnection and disinterested 'information hubs' rather than as political participants.[8] As such, they actively elude political accountability (and, in the case of ENISA, engagement with academic researchers).

The integration of commercial participants and absorption of commercial logics is another way in which the multivalent framework of cybersecurity takes shape. Through public-private dialogues and platforms, private sector participants are drawn into internet security governing, and authorized to act in its name (DeNardis, 2012). This cooperation takes shape in ad-hoc and indeed hesitant manner, exemplifying the tension between fixing and flexing in resilience governance strategies. Private companies want clear rules for everyone – so that there is a 'level playing field' – but they are to be kept within the desired limits of governmental intervention. Public actors desire ambiguity and flexibility for intervention, and hope to transfer responsibility to the private sector and the idealized private culture of creativity, innovation, and flexibility. But the commercial logic in cybersecurity operates at a more fundamental level than the fostering of private sector cooperation. The formal legal basis of the Cybersecurity Directive proposed in 2013 is made up of the legal provisions concerning functioning of the European internal market (in 't Veld, 2013; European Commission, 2013: 8). The logic of market integration becomes written into the security code here, while simultaneously the security logic of protecting infrastructures becomes part of market rationale.

The bureaucratic translation of vitalism thus appropriates some elements of resilience-thinking while discarding others. Cybersecurity's attempt to mimic the vital system it seeks to secure entails a

'flawed translation' whereby ideals of flexible governing and self-organization collide with bureaucratic practices and hierarchical rationalities. This translation can be further teased out by examining the important and growing agenda of trans-European cyber-exercises, one of ENISA's more prominent tasks. For Walker and Cooper (2011: 151), the scenario and the exercise are paradigmatic modes of 'non-predictive futurological' knowledge techniques within contemporary strategies of resilience and 'adaptive risk management' (also Lakoff, 2007; Aradau and van Munster, 2011). The first pan-European cyber-exercise took place in 2010 and involved the active participation of 22 member states and observance by eight states. In 2011, the first joint EU–US exercise took place under the name of 'Cyber Atlantic'. Through exercises, practitioners seek to anticipate the unknown, identify weaknesses, and generate cross-boundary interconnections between the distributed elements of a European cybersecurity space (ENISA, 2009: 14–15). Perhaps most importantly, the scenario is a futurological knowledge technique that explicitly seeks to have a bearing on the *present*: the objective is to 'turn anticipation into action' (Godet and Roubelat, 1996: 166; cf. Amoore, 2011).

Despite their stated orientation to surprise and the anticipation of unknown futures, recent European cyber-exercises illustrate how the vitalist ambitions of cybersecurity agendas remain locked in bureaucratic rationality and organizational linearity. This begins with the narratives of recent cyber-exercises that enact dystopian futures in which perceived threats from criminal exploitation of the internet, on the one hand, and sophisticated forms of digital dissent, on the other, have become morphed (Wall, 2008: 873–4). These recent scenario narratives deploy thinly veiled resemblances to political anxieties about the contemporary landscape of dissent. CyberAtlantic 2011 worked with a so-called 'advanced persistent threat' scenario, in which a hacker group called 'Infamous' leaked sensitive European documents online through a 'Euroleaks website'.[9] By comparison, CyberEurope 2010 enacted a scenario whereby Europe came 'under attack' from a 'cyber-criminal', leading to an emergency situation in which Europe's 'entire logistics chain [was] severely disrupted'.

> ... no banking and online business services can currently be performed. Pharmacies in several countries are unable to expedite prescriptions and newspapers cannot be printed as they are dependent on an active internet connection. ... Many critical social functions are threatened. (ENISA, 2011c)

The attack was scripted to be perpetrated by a group calling itself the 'Funk Mercenaries' – a dystopian European imagination in which the boundaries between cyber-crime and hacktivism have become completely

blurred. In the scenario, the Funk Mercenaries release the following statement:

> while Internet has been developed to enhance sharing and cooperation at all levels, it has actually led to exaggerate the differences, widen the gap and finally force separation between European peoples. This social clustering is reflected on the European Internet's infrastructure: no resilience at all. We, the Funk Mercenaries, will take you on a journey to prove it. Today, you will time travel back to the 1960s. (ENISA, 2011c)

The narrative fiction of the scenario and the not-quite-realistic newsflashes function to draw in the players affectively: to keep them, in the words of one exercise planner, 'busy . . . and happy'.[10] At the same time, however, experts emphasize that scenarios have to be 'plausible' and have to relate rationally to present conditions (ENISA, 2009: 23).[11]

The actual unfolding of the cyber-exercise entails a curious balance between the open-endedness of scenarios and response on the one hand, and the rationally expected player actions and scripted objectives on the other. The scenario deliberately creates a 'fog of war' through uneven and cryptic information injects that challenge participants to respond creatively and establish unexpected connections (Adey and Anderson, 2011: 2891). CyberStorm, for example, involved a scenario of attack by an activist group that launched a computer worm. False information was deliberately injected during the scenario, so that 'you could not trust information, there was wrong information placed on social networks.... People didn't know if they could trust information anymore.'[12] Scenario planners keep an open mind about the reactions their players will display, and use multiple pathways to inject information into the exercise. On the other hand, however, exercise participants are not to become *too* creative and playful. Expected player response is scripted and discussed in advance of running a scenario, and the perceived rationality of such responses is considered to be important. For example, scenario planners seek expert advice on 'realistic' responses that private participants and computer companies could display during a crisis and ask, 'Would this happen more or less in real life?'[13]

During the CyberEurope exercise, one of the main challenges was perceived by the planners to be the question of how to keep all participants to the script. Players were expected to respond rationally and in the *right* way to specific information 'triggers', and they were at times nudged in the right direction when interpreting the fictional information (ENISA, 2011a: 24). As one exercise planner put it in his evaluation of the exercise: 'the only thing I had to do was to sometimes help the players in the right direction. And to make sure that they did not start their own play' (ENISA, 2011c). Thus, CyberEurope 2010 exhibited a tension

between the appeal to future emergency and fluid response on the one hand (Anderson and Adey, 2012: 24), and the desire to play out a transcendental script and display the right modes of response on the other. In practice, these cyber-exercises operate less as imaginative tactics geared toward surprising and unpredictable futures and more as a method of generating bureaucratic interconnections and banal practices – for instance, a CERT worker in Rome knowing whom to call in Warsaw if service disruptions rippled across borders, or which binder to pull off the shelf in a cascading event.

Scenario planning is, on the one hand, a paradigmatic technique for acting on uncertain futures and 'stimulating the imagination'. But it is also a tool for '*disciplining* the imagination', which 'must relate rationally to the way people could behave' (Khan, 1962: 145, emphasis added). ENISA's *Good Practice Guide* for cyber-exercises offers a strict procedural template to be implemented in member states, and outlines a tightly-drawn exercise lifecycle, which sets out an ordered linear process of determining objectives, exercise planning, scenario design and practical scheduling. This process is to be hierarchically managed by groups of 'organizers', 'planners', 'monitors' and 'participants'. Paradoxically, the exercise template seeks to produce a rational standard method for encountering and producing outcomes that are non-standard and unexpected. Cyber-scenarios have one pre-scripted 'truth' that players need to 'discover', and thus remain wedded to an epistemology of truth and reason. As such, they fail to transcend present registers of rationality and hierarchy. The profound respect for ignorance that for Greco is vitalism's key contribution to science is discarded in its bureaucratic translation in favour of the transcendent rationality of the threat script.

At the same time, scenarios and exercises as deployed within the European information security agendas work to assemble European security spaces and produce effects in the cyber-milieu in particular ways. Their bureaucratic logics come to revolve more around demonstrating preparedness 'to... customers, partners and regulators' than they revolve around confronting the truly contingent (cf. Clarke, 1999; Amoore and Hall, 2010; Aradau, 2010). Thus, they work to infuse mundane bureaucratic practices with an orientation toward everyday emergency, through the production of professional knowledge, protocol, and guidelines. These are to a large extent geared toward replicating the flow and interconnectivities of the ecosystem that they perceive themselves to be securing. The objectives and targets of CyberEurope 2010, for example, were assessed primarily through the extent to which the exercise succeeded in fostering connections, communications and standardizations in relation to potential cyber-incidents (ENISA, 2011a: 32–8). The exercise emphasized continued information circulation, and monitored and mapped the alternative communications flows that emerged once specific online channels broke down.[14] One explicit ambition of the

exercise was the integration of emergency planning into the daily bureaucratic routine, because 'if the scenario had occurred in real life', as the evaluation report notes, 'players would also have had to deal with their ordinary tasks' (ENISA, 2011a: 24).

Contra the establishment of supranational competences, European security space is here forged through technical interconnectivities, data interoperability and the mobilization of webs of communication. So, for example, under the Framework Decision on Attacks Against Information Systems, member states have the obligation to respond to urgent requests for information from other member states through points of contact that are available seven days a week, 24 hours a day.[15] In the words of one Commission interviewee, this creates the means of getting hold of data outside 'the regular channels' which would involve 'an official request and [would] . . . take . . . weeks or months'.[16] Cybersecurity, in this sense, produces a European security space through 'governing the interstices' of 'a Europe of cracks and fissures, a leaking Europe in which streams of potential risks, hazards and threats seep through the governmental body' (Walters and Haahr, 2005: 106). The orientation of bureaucratic practice toward potential cyber-emergencies seeks interconnectivity and interoperability that could stitch together European security space.

Ultimately, bureaucratic vitalism and its desires for interconnectivity are mobilized in the name of a particular European 'way of life'. If it is 'life more than the law' that has become the 'issue of politic[s]' here (Foucault, 1998: 145), a question arises concerning the vision of life enacted and produced through the cybersecurity agenda. The extent to which future life in Europe is envisioned to require online connectivity and cyber-literacy is striking. The European digital economy is not just intimately tied to Europe's economic future but becomes a prerequisite for social and political participation. Fostering cyber-technology and internet literacy in Europe firmly connects economic ambitions to a way of life 'where every European can fully express his or her economic and social potential' (European Commission, 2011: 3). The agenda of interconnected economic, social, and political life, of making 'every European digital', is stitched to the potential for cyber-emergency to disrupt and disconnect the vital networks of this European way of life. The projected imperative of the interconnected life engenders a banal, everyday, potential emergency without events – a bureaucratic translation of the vital.

Concluding Reflections

Security practices mobilized around the interconnected emergency want to move beyond predictive calculation and seek to turn 'crisis response into a strategy of permanent, open-ended responsiveness' (Walker and

Cooper, 2011: 154). We offer the notion of bureaucratic vitalism to capture the way in which the European bureaucracy translates and redeploys the language and knowledge frames of vitalism and complexity without producing a fully felicitous translation. Mundane practices oriented to surprise and the event do not fully mirror the emergent elements they perceive themselves to be acting upon. Instead they produce an everyday orientation to emergency that preoccupies itself with the establishment of knowledge, procedure and narrative in the face of the event that cannot be avoided.

The everyday orientation of bureaucracy to complex crisis deploys an impoverished sense of contingency – it seizes upon a notion of the incipient and unpredictable in the name of emergent governing, but ultimately requires the restoration of the transcendental script of an event and a protocol of 'right' responses that are thought compatible with crisis in the 'real world'. In this sense, the flawed translations whereby resilience thinking becomes a template for bureaucratic governing appropriate certain elements of vitalism, such as the imperative of movement over structure and the ideals of decentred connectedness. But, significantly, they also discard elements, most importantly vitalism's valuation of ignorance and its profound attachment to indeterminacy. In this sense, resilience becomes a 'paradigm' of governing that 'comes in to replace another' *without*, in Greco's words (2005: 24), 'affecting what is understood to be the ethos of scientific knowledge and its relation to the world'.

To paraphrase Stengers (1997: 17), the intrinsic complexity of vital systems makes for 'risky' decisions in knowledge production and experimentation (as in the exercise) and 'the ever-present risk of "silencing" the very thing one is interrogating'. Rather than accepting the proclamations of a vitalist security apparatus that says it is able to avoid reduction and the limits of predictive knowledge, the task is to be attendant to the faltering practices of appropriating and translating complexity thinking. In other words, cyber bureaucrats may not be doing what they say they are doing, but they produce effects and shape the way security politics play out – particularly as actual or projected crises are seized upon in moments of uncertainty. Braun argues that politics is about 'the *determination* of incipient events, the on-going and ever renewed work of turning contingency into necessity' (2011: 392). What matters are the ways in which the contingent is seized upon, which 'throws us forward into yet another such moment, and another and another' (p. 392). This process of turning contingency into necessity is precisely the place of politics in fashioning the interconnected emergency. Whilst the conceptual frame of complex security domains seem to be moulded around depoliticized notions of vitality and resilience, in practice they actively shape determinations of the cyber-milieu. This tension between the

embrace of contingency and its ultimate foreclosure in security governance is one of the key fault-lines in an emergent politics of complexity.

Acknowledgements

Many thanks to the special issue editors, Pete Adey, Ben Anderson and Steve Graham, for their encouragement of this work and their insightful comments. Many thanks also to the anonymous reviewers of *TCS*, and to Melinda Cooper, Luis Lobo-Guerrero, John Grin, Marijn Hoijtink, Samuel Randalls, Ute Tellmann, and Floris Vermeulen for their very helpful comments on earlier versions of this paper. Financial support for this research was provided by the Dutch Council for Scientific Research (NWO), through the VIDI-grant *European Security Culture*, award number 452-09-016.

Notes

1. Other authors have made similar moves to conceptualize 'environmental' modalities of power (Massumi, 2009) in contemporary contexts. See, for example, Melinda Cooper's work on the frontiers of biotechnology (2008) and Ben Anderson's work on 21st-century US counterinsurgency operations (2011).
2. ARPA is a research and development agency that is itself defined by an orientation toward the surprising. With a motto of 'Creating and Preventing Strategic Surprise', the agency is tasked with 'high risk–high payoff' research of forward-thinking technological developments beyond those that might emerge from more orthodox military agencies. ARPA's key operational mandate is to manipulate the unexpected, and the technologies that led to the development of ARPANET were geared toward these ends of 'creating surprise rather than seeking to avoid it' (Van Atta, 2008: 25).
3. This does not mean that there are no attempts to reign in and delimit internet openness. The 2012 meeting of the UN-based International Telecommunication Union revealed this tension between openness and restriction. The meeting was set to review the International Telecommunications Regulations and it was widely cited as a battle between 'East and West' over the proponents of more centralized control and more stringent cybersecurity regulations from countries like Russia and China and market-driven approaches led by the US and the EU (Kiss, 2012). Further complicating matters are the host of other content and copyright initiatives like ACTA, PIPA, and SOPA that push for restricting information openness.
4. Interview, National Cyber Security Centre official, The Hague, 23 April 2012.
5. ENISA phone interview, 14 February 2012.
6. Comments made during the *Hearing on Cyber Attacks against Information Systems, European Parliament*, 4 October 2011, http://www.europarl.europa.eu/document/activities/cont/201110/20111010ATT28827/20111010ATT28827EN.pdf
7. Member states have 'to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor' (Council of the European Union, 2005).

8. Europol interview, The Hague, 12 March 2013.
9. ENISA, 'Cyber Atlantic 2011: First Joint EU–US Cyber Exercise', Powerpoint slides, p. 6. Available at: http://www.bic-trust.eu/files/2011/12/slides15.pdf
10. ENISA phone interview, 14 February 2012.
11. Interview, National Cyber Security Centre, The Hague, 23 April 2012.
12. Interview, National Cyber Security Centre, The Hague, 23 April 2012.
13. Interview, National Cyber Security Centre, The Hague, 23 April 2012.
14. Steve Purser, comments made during the Hearing on Cyber Attacks against Information Systems, European Parliament, 4 October 2011.
15. Steve Purser, comments made during the Hearing on Cyber Attacks against Information Systems, European Parliament, 4 October 2011.
16. Interview, European Commission Information Society Directorate, Brussels, 16 April 2012.

References

Abbate J (2000) *Inventing the Internet*. Cambridge, MA: MIT Press.
Abrahamsson C (2012) Mathematics and space. *Environment and Planning D: Society and Space* 30(2): 315–321.
Adey P and Anderson B (2011) Event and anticipation: UK civil contingencies and the space-times of decision. *Environment and Planning A* 43: 2878–2899.
Amoore L (2008) Consulting, culture, the camp: On the economies of the exception. In: Amoore L and de Goede M (eds) *Risk and the War on Terror*. London: Routledge.
Amoore L (2011) Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6): 24–43.
Amoore L and Hall A (2010) Border theatre: On the arts of security and resistance. *Cultural Geographies* 17(3): 299–319.
Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34: 777–798.
Anderson B (2011) Facing the future enemy: US counterinsurgency doctrine and the pre-insurgent. *Theory, Culture & Society* 28(7–8): 216–240.
Anderson B and Adey P (2012) Governing events and life: 'Emergency' in UK civil contingencies. *Political Geography* 31: 24–33.
Ansell C, Boin A and Keller A (2010) Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management* 18(4): 195–207.
Aradau C (2010) The myth of preparedness. *Radical Philosophy* 161: 2–7.
Aradau C and van Munster R (2011) *Governing Catastrophe: Genealogies of the Unknown*. London: Routledge.
ARECI (2007) *Availability and Robustness of Electronic Communications Infrastructures: The ARECI Study*. Brussels–Luxembourg: ECSC-EC-EAEC.
Baran P (1964) *On Distributed Communications I: Introduction to Distributed Communications Networks*. Santa Monica: The RAND Corporation.
Barnard-Wills D and Ashenden D (2012) Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture* 15(2): 110–123.
Barry A (2001) *Political Machines: Governing a Technological Society*. London: The Athlone Press.

Barry A (2010) Materialist politics: Metallurgy. In: Braun B and Whatmore SJ (eds) *Political Matter: Technoscience, Democracy and Public Life*. Minneapolis: University of Minnesota Press.
Barry A and Walters W (2003) From EURATOM to 'complex systems': Technology and European government. *Alternatives* 28: 305–329.
Bennett J (2009) *Vibrant Matter: A Political Ecology of Things*. Durham: Duke University Press.
Betz DJ and Stevens T (2013) Analogical reasoning and cyber security. *Security Dialogue* 44(2): 147–164.
Braun B (2011) Book review forum: Jane Bennett, *Vibrant Matter: A Political Ecology of Things*. *Dialogues in Human Geography* 1(3): 390–405.
Canguilhem G (2009) *Knowledge of Life*, trans. Geroulanos S and Ginsburg D. New York: Fordham University Press.
Clarke L (1999) *Mission Improbable: Using Fantasy Documents to Tame Disaster*. Chicago: University of Chicago Press.
Cohen JE (2007) Cyberspace as/and space. *Columbia Law Review* 107(1): 210–256.
Cooper M (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle: University of Washington Press.
Cooper M (2010) Turbulent worlds: Financial markets and environmental crisis. *Theory, Culture & Society* 27(2–3): 167–190.
Council of the European Union (2005) *Council Framework Decision on Attacks against Information Systems*. Brussels, 24 February (2005/222/JHA).
Council of the European Union (2008) *Directive on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection*. Brussels, 22 May (9403/08).
Crampton J (2003) *The Political Mapping of Cyberspace*. Chicago: University of Chicago Press.
Deibert RJ (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium* 32(3): 501–530.
Deibert R and Rohozinski R (2010) Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology* 4(1): 15–32.
Deibert R, Rohozinski R and Crete-Nishihata M (2012) Cyclones in cyberspace: Information shaping and denial in the 2008 Russian-Georgian war. *Security Dialogue* 43(1): 3–24.
DeNardis L (2009) *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.
DeNardis L (2012) Hidden levers of internet control: An infrastructure-based theory of internet governance. *Information, Communication & Society* 15(5): 720–738.
Den Boer M, Hillebrand C and Nölke A (2008) Legitimacy under pressure: The European web of counter-terrorism networks. *Journal of Common Market Studies* 46(1): 101–124.
Dillon M (2007) Governing terror: The state of emergency of biopolitical emergence. *International Political Sociology* 1(1): 7–28.
Dillon M and Lobo-Guerrero L (2008) Biopolitics of security in the 21st century: An introduction. *Review of International Studies* 34(2): 265–292.
Dillon M and Reid J (2009) *The Liberal Way of War: Killing to Make Life Live*. London: Routledge.

Dodge M and Kitchin R (2011) *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press.
Dunn M (2005) The socio-political dimensions of critical information infrastructure protection. *International Journal of Critical Infrastructures* 1(2/3): 258–268.
ENISA [European Network and Information Security Agency] (2009) *Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks*. Heraklion. Available at: www.enisa.europa.eu (accessed September 2013).
ENISA [European Network and Information Security Agency] (2011a) *Cyber Europe 2010 – Evaluation Report*. Heraklion. Available at: www.enisa.europa.eu (accessed September 2013).
ENISA [European Network and Information Security Agency] (2011b) *Inter-X: Resilience and the Internet Interconnection Ecosystem. Summary Report*. Heraklion. Available at: www.enisa.europa.eu (accessed September 2013).
ENISA [European Network and Information Security Agency] (2011c) *CyberEurope 2010* (Report – Video), 20 April. Available at: http://www.podcast.tv/video-episodes/enisa-cyber-europe-2010-report-video-14464257.html (accessed September 2013).
European Commission (2004) *Critical Infrastructure Protection in the Fight against Terrorism*. Brussels: COM (2004) 702 final.
European Commission (2009a) *Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience*. Brussels: COM (2009) 149 (30 March).
European Commission (2009b) *Workshop on the Establishment of a European Public-Private Partnership for Resilience*. Brussels, 17 June.
European Commission (2010a) *A Digital Agenda for Europe*. Brussels: COM (2010) 245 final/2 (26 August).
European Commission (2010b) *Establishment of a European Public-Private Partnership for Resilience* (EP3R). Version 2.0, 23 June.
European Commission (2011) *Critical Information Infrastructure Protection: Achievements and Next Steps: Towards Global Cyber-Security*. Brussels: COM (2011) 163 final (31 March).
European Commission (2013) *Proposal for a Directive concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*. Brussels: COD (2013) 0027 (7 February).
European Forum for Member States (2011) *European Principles and Guidelines for Internet Resilience and Stability*. Available at: http://ec.europa.eu (accessed September 2013).
Foucault M (1994) *The Order of Things: An Archeology of the Human Sciences*. New York: Vintage.
Foucault M (2007) *Security, Territory, Population: Lectures at the Collège de France 1977–1978*, trans. Burchell G. New York: Palgrave.
Fraser M, Kember S and Lury C (2005) Inventive life: Approaches to the new vitalism. *Theory, Culture & Society* 22(1): 1–14.
Galison P (2001) War against the center. *Grey Room* 4: 5–33.
Greco M (2005) On the vitality of vitalism. *Theory, Culture & Society* 22(1): 15–27.

Grubesic TH and Murray AT (2006) Vital nodes, interconnected infrastructures, and the geographies of network survivability. *Annals of the Association of American Geographers* 96(1): 64–83.
Hansen L and Nissenbaum H (2009) Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly* 53: 1155–1175.
In 't Veld S (2013) Public comments at the Annual Computers, Privacy and Data Protection Conference, Brussels, 23–4 January.
Kiss J (2012) ITU and Google face off at Dubai Conference over future of the internet. *The Guardian*, 3 December.
Kroes N (2012) Public-private cooperation in cyber-security. Speech delivered to the Security and Defence Agenda, Brussels, 30 January. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/47&format=HTML&aged=0&language=EN&guiLanguage=en (accessed September 2013).
Kuus M (2011) Bureaucracy and place: Expertise in the European quarter. *Global Networks* 11(4): 421–439.
Lakoff A (2007) Preparing for the next emergency. *Public Culture* 19(2): 247–271.
Lakoff A and Collier S (2010) Infrastructure and event: The political technology of preparedness. In: Braun B and Whatmore SJ (eds) *Political Matter: Technoscience, Democracy and Public Life*. Minneapolis: University of Minnesota Press.
Larner W (2006) Neoliberalism: Policy, ideology, governmentality. In: de Goede M (ed.) *International Political Economy and Poststructural Politics*. Basingstoke: Palgrave.
Lash S (2006) Life (Vitalism). *Theory, Culture & Society* 23(2–3): 323–349.
Little RG (2002) Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructure. *Journal of Urban Technology* 9(1): 109–123.
Lundborg T and Vaughan-Williams N (2011) Resilience, critical infrastructure and molecular security: The excess of 'life' in biopolitics. *International Political Sociology* 5(4): 367–383.
Lute JH (2012) Keynote address at 'Transatlantic Dimensions of Cyber Security', Center for Strategic and International Studies, Washington, DC. Available at: http://csis.org/multimedia/video-transatlantic-dimensions-cyber-security-keynote-speakers-cecilia-malmstroem-and-jan (accessed September 2013).
Mackenzie A (2005) The performativity of code: Software and cultures of circulation. *Theory, Culture & Society* 22(1): 71–92.
Malmström C (2011) Making cyberspace more secure. Speech delivered at the Security and Defence Agenda conference, 'Defining Cyber Security', Brussels, 9 November.
Massumi B (2009) National enterprise emergency: Steps toward an ecology of powers. *Theory, Culture & Society* 26(6): 153–185.
Mueller M (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.
North Atlantic Treaty Organization (2010) *NATO 2020: Assured Security, Dynamic Engagement*. 17 May. Available at: http://www.nato.int/cps/en/natolive/official_texts_63654.htm (accessed 5 December 2014).

Oerting T (2013) Public comments at the Annual Computers, Privacy and Data Protection Conference, Brussels, 23–4 January.
Perrow CB (1999) *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press.
Raley R (2009) *Tactical Media*. Minneapolis: University of Minnesota Press.
Reid J (2006) *The Biopolitics of the War on Terror*. Manchester: Manchester University Press.
Reid J (2012) The disastrous and politically debased subject of resilience. *Development Dialogue* 58: 67–80.
Roberts S, Secor A and Zook M (2012) Critical infrastructure: Mapping the leaky plumbing of US hegemony. *Antipode* 44(1): 5–9.
Servida A (2009) Towards a EU policy on critical information infrastructure protection. Paper delivered at TERENA 26th TF-CSIRT Meeting, Riga, Latvia, 19–20 January.
Stengers I (1997) *Power and Invention: Situating Science*. Minneapolis: University of Minnesota Press.
Thrift N and French S (2002) The automatic production of space. *Transactions of the Institute of British Geographers* 27(3): 309–335.
Urry J (2003) *Global Complexity*. Cambridge: Polity.
Van Atta R (2008) Fifty years of innovation and discovery. In: *DARPA: 50 Years of Bridging the Gap*. Washington, DC: US Government Printing Office.
Wall D (2008) Cybercrime and the culture of fear. *Information, Communication and Society* 11(6): 861–884.
Walker J and Cooper M (2011) Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue* 42(2): 143–160.
Walters W and Haahr JH (2005) *Governing Europe: Discourse, Governmentality and European Integration*. New York: Routledge.
World Economic Forum (2011) *Global Risks 2011*, 6th edn. Geneva: World Economic Forum.
Zittrain J (2009) *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press.

Stephanie Simon is a Lecturer at the University of Amsterdam. Her research focuses on security, control and spatiality in cities and transnational contexts. Her work has been published in *Antipode*, *Journal of Urban Cultural Studies*, *Security Dialogue, Social and Cultural Geography,* and *Space and Polity*.

Marieke de Goede is Professor of Political Science at the University of Amsterdam. Her research focuses on issues of risk, speculation and post-9/11 security culture. She is author of *Speculative Security: the Politics of Pursuing Terrorist Monies* (University of Minnesota Press, 2012) and editor, with Louise Amoore, of *Risk and the War on Terror* (Routledge, 2008). She is an Associate Editor of *Security Dialogue*.

This article is from a TCS Special Issue on Governing Emergencies (32.2, March 2015), edited by Peter Adey, Ben Anderson & Stephen Graham.