2 Cyberwar’s Subjects

INTERPELLATIONS AND ENTICEMENTS

In wars in Syria, Ukraine, and elsewhere, it is common for soldiers to be contacted on their mobile phones by the enemy, with messages either seductive (“I’ll send you my photo,” “When is your birthday?”[1]), to inveigle the release of tactical intelligence, or derogatory (“You’re nothing but meat to your commanders!” “Your body will be found when snow melts”[2]), to demoralize and terrorize. These messages are far from state-of-the-art digital influencing mechanisms, but, bold and crude, they combine the atavistic directness of ideological recruitment and intimidation with the newest technological means of individual subjectification. Yet, extreme as the conditions of these battlefield conversations are, they exemplify a far broader condition of the denizens of states, quasi-states, and would-be-states involved in conflicts waged across digital networks traversed by campaigns of propaganda, persuasion, and surveillance.

To analyze these conditions, we take as our point of departure the Marxist theorist Louis Althusser’s (1971) appropriation of Jacques Lacan’s ([1969–70] 2007) early work on the imaginary and symbolic orders. Althusser proposed that in capitalism, ideological state apparatuses (ISAs) generate social identity by “interpellating” or “hailing” subjects to engage them in an imaginary relation with the reality of their exploited condition. This proposition has informed a rich line of media studies analysis. However, recently, a number of theorists—Slavoj Žižek (1989, 1997a), Teresa Brennan (2004), Jodi Dean (2008, 2010), Samo Tomšič (2015), and others—have developed and revised this Marxist–Lacanian position to adapt it to the conditions of digital capitalism. In particular, they have emphasized the elements in Lacan's later thought that elaborate the connection between pleasure (however painful or pain inflicting) and a capitalist discourse that entices ever-unsatisfied subjects to labor, in various forms, in search of an enjoyment *(jouissance)* that is always frustrated by the operations of the very social order that sets it in motion (Lacan 2007, 80–81).

We pursue this line of analysis to investigate cyberwar as a new, personalized, yet far-reaching and border-perforating mobilization and discipline of populations. The sometimes-intentional but often-unwitting labor force of cyberwar, network users are interpellated as subjects by world-market states and would-be states to facilitate antagonisms, form alliances, and engage in cyberbattles in various ways, from DDoS attacks, hacking, and trolling to sharing, liking, or commenting. It is, however, an index of the mounting technological intensity of capital (in Marxist terms, its deepening "organic composition") that this process is increasingly automated, whether through the use of software bots to entice or harass or by the enlistment of the user's computer as weapon component. In these conditions, whatever new identities and alignments are proffered, cyberwar's subjects are also immediately rendered obscure and incomplete. The difficulty of attributing and verifying digital warfare operations conducted at internet speeds by machinic agents means that complicit user populations never know for sure what is going on, or what part they play within it, a disoriented condition that, however, only further encourages extreme compensatory identity assertions, virulent conspiracy theories, the consolidation of internet echo chambers, yet greater automation of surveillance to halt real or imagined automated intrusions and infiltration, and yet greater misrecognition by the subjects of cyberwar of their own exploitation and vulnerability.

APPARATUS, CYBERSPACE, NOMAD

When digital networks first diffused from their military point of origin out through society, they were widely greeted as an antidote to indoctrinating powers of state and corporations, a technology of freedom.

Even for those who never read Althusser, in spirit at least, the slogan was "NPCs [networked personal computers] are the antithesis of the ISAs." Many today are reluctant to give up this hope that digital networks are inherently liberatory, a position that has two variants, liberal and radical.

The liberal, originally libertarian, version was that of the North American digital counterculture (Markoff 2005; Turner 2006). Orbiting initially around points such as the early electronic bulletin boards of The WELL (The Whole Earth 'Lectronic Link), *Wired* magazine, and Stewart Brand's *Whole Earth Catalog,* it posited "cyberspace" as an autonomous realm beyond the reach of the state (Barlow 1996), overlooking, at first, and then dismissing, corporate surveillance that has been long intertwined with government surveillance in one powerful complex (Glaser 2018). Those who participated in this perspective were, of course, aware of the military origins of the internet; many had been involved in the anti–Vietnam War movement. But they believed networks had escaped the purview of the Pentagon to become a domain for new virtual identities and communities, a realm of psychological self-actualization. Strongly associated with small hacker start-up companies, this perspective was scornful of corporate suits and legacy media but by no means necessarily anticapitalist. On the contrary, networks often appeared as the fulfillment of the horizontalism of the market's invisible hand, stripped from the vertical accretions of state and monopolist power. Such network libertarianism would eventually be assimilated into neoliberalism, decomposing into a "Californian ideology" (Barbrook and Cameron 1996) that celebrated both the free authenticity of online communication and the Reaganite deregulation that proclaimed the dismantling of the state while funneling giant defense contracts to Silicon Valley. This position didn't so much contradict Althusser as move in a different universe, or at least one separated by an ocean, a continent, and three hundred years of political history. Such belief in the inherently emancipatory powers of the internet has, in its corporately co-opted form, circulated around the planet and remains an article of faith for many users in the age of Google and Facebook.

The radical account of the internet's counter to the ISAs was far more attuned to the issues addressed by Althusser. It in part issued from much the same European left milieu—at least if we accept that one of its basic texts was the extraordinary "nomadological" writings of philosopher Gilles Deleuze and antipsychiatrist Félix Guattari (1986). Their immediate point of reference is the ancient warfare of the nomadic steppe warriors made famous by Genghis Khan. Deleuze and Guattari characterize the culture of these mobile, decentralized nomad warriors as a "war machine"—but one independent from and opposed to any sedentary state formation and, hence, paradoxically separated from any notion of "war" as conventionally understood today. In their account, the fighting aspects of nomadism are subordinated to the transformative processes of "becoming" generated by the new assemblage of humans, horses, and metallurgy brought into being by nomad war. Such "war" is an activity that *precedes* the state and has to be appropriated by it to produce the systematized and rationalized violence we now know by that name.

Though Deleuze and Guattari focus their account of war machines on medieval nomads, they conclude with a reference to the late twentieth century. This, they admit, is an era that the state "war machine" dominates but, nonetheless, still contains possibilities for nomadic reappropriations of its technologies, creating new possibilities for dissenting, transgressive becoming. Whether they had in mind digital networks is impossible to tell, although Guattari's involvement with alternative media makes it likely: the connection is absolutely explicit in Deleuze's (1992) later, prescient "Postscript on the Societies of Control," which also recognized the rapid state appropriation of such powers. But others, such as Manuel DeLanda (1991), rapidly spelled out the affinity between their account of the decentralized, swarming, and rhizomatic nomadic war machine and packet-switching, many-to-many, digital "meshworks," with a potential to subvert the control of state masters. This idea was taken up by anarchists and autonomists associated with alterglobalism and its independent media centers, hacktivism and electronic civil disobedience, a political ambience that found its fullest articulation in the work of Guattari's friend and political ally Antonio Negri and his concept of an emergent revolutionary "multitude" armed by new technologies (Hardt and Negri 2000, 2017). In such accounts, networks appear not, as in the liberal version, just as an escape from the state but also as counterpower, militantly contesting it.

In the liberal view, the "electronic frontier" is a site where selfdetermining individuals escape from the tyranny of the state and establish communities with like-minded people whose adoption of virtual identities shrugs off socially imposed masks in a new digital authenticity. The radical view is that of a process that dissolves the individual subject in metamorphoses of decentered "divididuals" with new collective possibilities, drawing lines of flight that are simultaneously lines of fight against commanding power. Both, however, see digital networks undoing an ideological authority that polices entry into the world of symbolic communication. Both reflect a certain historical reality, the moment when digital networks, having spread from the US military complex into civilian use, develop without clear state regulation or model for commercial exploitation, as witnessed by the great dot-com crash of 2000. In this window of indeterminacy, all kinds of networked social experiments and political possibilities did indeed bloom.

The context of cyberwar is, however, very different. It is, for one, a context where capital has (in part by the capture of radical experiments) found a business model adequate to the exploitation of networks in the rationalization of "Web 2.0," with its user-generated content, algorithmically targeted advertising, and big data–sucking surveillance. And it is, as we have seen, one where increasingly, states, quasi-states, and their proxies, working through and with this new digital capitalism, strive to consolidate and exercise their monopolies of violence, one against another. Today both liberal and radical insistence on the antistatist valence of the digital networks mystifies and occludes what is unfolding in a way that can itself be termed ideological.

LEVÉE EN MASSE

The state reabsorption of the digital war machine can be tracked in the eager reading of Deleuze and Guattari's nomadological texts by U.S. defense intellectuals.[3] However, for our purposes, a more relevant historical analogy is that propounded by Audrey Cronin (2006), an American academic counterterrorism expert, in her widely discussed account of cyberwar as the new *levée en masse.* The *levée en masse* was the policy of military conscription adopted by the French state in the aftermath of the

Revolution of 1789 in a desperate attempt to counter the superiority of the professional ancien régime armies sent to crush it. It was unexpectedly successful. Numerically superior and (sometimes) fervent citizen-soldiers shattered the ranks of their opponents at Valmy and other battlefields. While a matter of state policy, *levée en masse,* as Cronin emphasizes, harnessed revolutionary popular enthusiasm; in French, *levée* signifies not merely a governmental imposition, such as a tax, but also an uprising. As Cronin (2006, 79) points out, it drew on the new means of transportation (good roads) and communication (cheap printing) of a nascent mercantile capitalism to recruit its soldiers and get them to the front. With the collapse of censorship, the circulation of revolutionary tracts, songs such as the "Marseillaise," and images, such as pictures of the storming of the Bastille, ensured that "the French populace was reached, radicalized, educated, and organized so as to save the revolution and participate in its wars."

Then Cronin draws her parallel with contemporary cyberwars. Pointing to the "global spread of Islamist-inspired terrorist attacks . . . the rapid evolution of insurgent tactics in Iraq, the riots in France, and well beyond," she argues that this is "the 21st century's *levée en masse,* a mass networked mobilization" (77). With her eyes on al-Qaeda and digital jihadism, she suggests that "democratization of communications, an increase in public access, a sharp reduction in cost, a growth in frequency, and an exploitation of images to construct a mobilizing narrative" are all working in favor of "so far uncontrollable insurgency" (81). Like the *levée en masse,* the evolving character of communications is "altering the patterns of popular mobilization, including both the means of participation and the ends for which wars are fought" (84–85). "Today's mobilization," she continues, "may not be producing masses of soldiers, sweeping across the European continent, but it is effecting an underground uprising whose remarkable effects are being played out on the battlefield every day" (85). "Cyber-mobilization" is bringing about broad "social, ideological, and political changes"; successfully harnessing these elements is "the key to advantage in future war." In the alarm modality of post 9/11 U.S. military thought, she declares that "the information age is having a transformative effect on the broad evolution of conflict, and we are missing it" (87).

Cronin's analysis came in the early days of the U.S. "war on terror." We know now what form the "counter-mobilization" (87) that she urged against Islamic militancy would take: mass surveillance, drone strikes, and Special Forces ops. Other aspects of cyberwar, such as its state versus state modalities, have subsequently come to the fore. However, her article retains its relevance because of the way it articulates a project of state recapture of an initially "revolutionary" force—the emergence of networked populations.[4] There is (and was) a deep political ambivalence in the concept of the *levée en masse,* one caught perfectly in the subtitle of Jean-Paul Bertaud's (1988) study *The Army of the French Revolution: From Citizen Soldiers to Instruments of Power.* The *levée* was indeed radical: it saved the Revolution. It then, however, became the basis for the triumphs of Napoleon's armies, in a project of conquest that founded a new and emphatically imperial power. It was also emulated and adapted by Napoleon's reactionary adversaries, providing a general war-making model for nineteenth-century, and then twentieth-century, great powers. Insofar as national conscription formed the basis for total war, a line connects Valmy to Verdun.

For Cronin, cyberwar is a matter of "mobilization." Geoffrey Winthrop-Young (2011, 134–35), discussing the military writings of Kittler, describes the category of mobilization well and makes the connection to issues of subjectivity:

> Mobilization erodes the boundaries between war and peace because it takes place in both; it erodes the boundary between the military and civilian population because it affects one as much as the other; and it erodes the distinction between material hardware and psychic software because it deals as much with the optimization of logistics, transport, and technology as with increasing mental preparedness and overall combat readiness. But what kind of human is most equipped (or least under-equipped) to deal with the acceleration and incomprehensibility of modern war? What kind of mind is available to make rapid, on the spot decisions, or even make up new rules when no fiat, no commanding authority, is in sight? What has been programmed to fight with a free will? The modern subject.

It could be argued that cyberwar, a form of highly technocratic warfare, is in some regards the opposite of the *levée en masse,* a type of war that, like nuclear weapons, frees states from their politically problematic dependence on mass armies. However, as we suggested in the previous chapter, this idea of cyberwar simply as a series of hacker-team exploits ignores the wider base of technosocial knowledge and practice on which such feats depend. It also ignores the global networked populations that cyberwar hacking traverses, targets, and exploits.

Hardt and Negri (2000) and others of the post-*operaismo* school have interpreted Marx's (1973) passing reference to a "general intellect" as an allusion to the collective skills, aptitudes, and identities necessary for capitalism's ceaselessly innovative technological development. Much the same logic applies to its concomitant development of technowar, a dynamic in which the "general" in "general intellect" could be taken as referring not only to a collective or communal process but one under military command! If we restore this process to view, the concept of mobilization, including the formation of specific subjectivities for cyberwar, makes sense, although it is a mobilization that, as we will argue later, is as much concerned with activating machines as it is with galvanizing users.

It is a form of mobilization that has novel features. Competing states have always engaged in usually clumsy and ineffective propaganda wars aimed at disaffecting their opponents' populations. On a networked planet, however, it is not just the homeland state that interpellates its subjects with the exceptional intimacy and intensity afforded by digital systems but also the enemy—the adversary state—that can do so. Before we develop these arguments further, we will give two examples of cyberwar mobilization. In both cases, we see how an initial revolutionary or insurgent use of the internet is appropriated by state apparatuses, those that emerge from the initial rebellion *and* those that seek to quell it or initiate new revolts against its outcomes. This dynamic leads to an escalating militarization of networks and the intensifying formation of warring data subjects. The first example involves conflict in Ukraine, the second in Gaza.

In Ukraine, the 2013–14 uprising of the Maidan against the Yanukovych oligarcho-kleptocratic regime, a classic "Facebook revolution," brought to power the government of President Poroshenko. Four years after, at the moment of writing this book, the new president himself is a center of several large scandals—from the disclosure, by the Panama Papers leak, of his secret offshore company, Prime Asset Partners Ltd, in the

British Virgin Islands, set with the goal of tax evasion (Harding 2016), to his lavish, half-million-dollar secret trip to Maldives at the beginning of January 2018 under the name of "Mr. Petro Incognito (Ukraine)," abandoning the country at war (Romanyshyn 2018b), since 2014, against pro-Russian separatists supported by the Russian military in the self-proclaimed Donetsk People's Republic (DPR) and Lugansk People's Republic. This is variously termed a *proxy war* (in the international and some Ukrainian media, emphasizing major Russian assistance to the separatists), *civil war* (by the Russian government and in many Russian media, emphasizing the division of Ukraine's population to deny the presence of the Russian troops), *antiterrorist operation* (ATO) (by the Ukrainian government until February 2018), and *armed aggression* (by the Ukrainian government since February 2018).[5]

Both sides, but especially pro-Russian forces, have made use of digital networks for computational propaganda over social media, digital espionage and hacking, ranging from DDoS attacks to the blackout of a major section of Ukraine's electric grid, launched from a Russian IP address. The Ukrainian side often mirrors the propaganda methods and tactics of the northern neighbor; for example, a Ukraine-based private English-language satellite television channel, Ukraine Today (2014–16), was modeled on Russia Today, insisting on the distinction between "good" and "bad" propaganda. The conflict has been characterized by widespread dissemination of doctored videos and disputed interpretations of critical events (such as the shooting down of Malaysia Airlines flight 17 over Donbas) fought out over social media.[6] There is substantial evidence that reporting on the conflict, in Ukraine, in Russia, and abroad, has been targeted by paid internet "trolling" enterprises located in Russia, tasked with intervening in discussions to depict Ukraine governments as fascist, incompetent, and corrupt, a puppet state of the degenerate, "gay" Western liberal democracies, and Ukrainians as the manipulated victims of imperialist designs to divide them from their Slavic Russian brothers (Sindelar 2014; Chen 2015; Patrikarakos 2017; Soshnikov 2017). This is accompanied by the circulation of faked war videos and fabricated atrocity stories (whose spurious nature, of course, doesn't preclude the existence of real war horrors and atrocities).

For its part, the Ukrainian government has, with the assistance of NATO consultants and advisors, mounted its own information war campaigns. Facebook and other social media platforms are widely used by civil-society organizations supplying Ukrainian troops and militia in the "Anti-Terrorist Operation Zone" (Patrikarakos 2017). Ukrainian hackers, volunteers or government employed, hack information from the CCTV cameras in eastern Ukraine, as well as local insurgents' bank accounts, phone conversations, and emails. Some hackers give information to the Peacemaker (Миротворец) website, indirectly associated with Ukrainian government figures who, in an appropriation of "leak and hack" tactics, call themselves "the friends of Assange" (Миротворец, n.d.). The site offers "information for law enforcement authorities and special services about pro-Russian terrorists, separatists, mercenaries, war criminals, and murderers." Peacemaker published information on nine thousand alleged "terrorists" fighting in Ukraine, calling for an open hunt for these people online and off. Shortly after the site's launch in early 2015, it came to public attention for publishing the personal details of forty-five hundred journalists, complete with phone numbers and emails. The website's creators accused them of collaborating with the "terrorists" because they had received accreditation from the leadership of the DPR.[7]

Both during the Maidan rebellion and the Donbas war, social media usage in Ukraine has split between rival platforms in a way broadly mirroring political divisions. While supporters of the Maidan revolution favored Facebook, and widely used it to coordinate and circulate news of their revolt, the majority of pro-Russian Ukrainians have congregated on VKontakte. Also known as VK (http://vk.com/), VKontakte is a Russian-owned social media platform, founded by Russian entrepreneur Pavel Durov in 2006, that, in its "user interface and functionalities . . . largely resembles Facebook," allowing a user to create a profile (public or private) and then start "'friending' other users" (Gruzd and Tsyganova 2014, 124). In January 2014, after Durov's refusal to turn over data on Ukrainian protesters to the Russian government, the founder was forced to sell his stake in the company to the company controlled by Russian oligarch Alisher Usmanov, a co-owner of Russia's second largest mobile telephone operator, MegaFon, and co-owner of the Mail.ru group, the largest Russian-speaking internet company. Meanwhile, Durov himself had to escape the country. While VK lacks Facebook's global reach, it has more than 100 million users, mostly from former Soviet republics. In Ukraine, VK is—or was—less popular than Google and YouTube but more so than Facebook. On May 2017, however, President Poroshenko announced a ban on VK and several other Russian-owned internet firms: Odnoklassniki, another widely used social network; Mail.ru, one of the country's most popular email services; Yandex, a major search engine; and software from Russian cybersecurity firm Kaspersky. The president described the measures as "an answer to 'massive Russian cyberattacks across the world'"; Ukrainian officials said that the social networks in question were "used to spread Russian propaganda, and that users' data are collected by Russia's secret services" (*Economist* 2017c). The decision was widely protested in Ukraine, but in the month following, Ukrainian Facebook accounts surged by around 2.5 million. After announcement of the ban, Ukraine's presidential administration claimed that its website had come under attack by Russian hackers.

Our second example of digital mobilization comes from the escalating network conflict between Israel and Palestine that has accompanied successive rounds of asymmetrical fighting in Gaza. In his *War in 140 Characters,* David Patrikarakos (2017) suggests that Israeli success in suppressing successive Palestinian intifada (uprisings) from the late 1980s on was based not only on massive military superiority but also on success in controlling framing and narration of the conflict in the international press. Israel's ability to restrict journalist access to the West Bank and Gaza, its cultivation of a relatively narrow and predictable range of foreign news channels, and the widespread sympathy to Israel in liberal public opinion, especially in the United States, all allowed the issue to be represented as a battle against terrorism. However, with the growing Palestinian use of the internet, and then of social media, this dominance is eroded.

From 2000, despite limited access and disrupted electricity supply, the internet became a means for Palestine's diasporic communities, both in Middle Eastern refugee camps and beyond, to share symbols and texts of national identity, a process referred to as an electronic or "cyber intifada" (Aouragh 2003). In the first Gaza War in 2008, designated by Israel as Operation Cast Lead, Israeli Defense Forces (IDF) restricted Western journalists' access to the war zone, resulting in a stream of images, video, and information relayed from the Gaza Strip to media outlets such as Al Jazeera and Al Arabiyya. The proliferation of Web 2.0 services allows the people of Gaza to upload detailed accounts to blogs, Twitter, YouTube, and, notably, Flickr, revealing scenes of "chaotic horror" caused by Israeli air strikes (Taylor 2012). In response, the IDF rapidly assembled a Spokesperson's Unit to produce a social media presence, but, despite persuading YouTube to take down some Palestinian videos, it had limited success. The deterioration of Israel's media position intensified in 2010 with the Mavi Marmara incident. The IDF's interception of a "peace flotilla" of boats breaking the economic blockade on Gaza culminated in an airborne assault on the main vessel, killing nine Turkish activists and wounding many others. Despite the IDF's attempt to block the ship's electronic communication, enough video and audio material was transmitted to convey the violent mayhem of the attack, creating a diplomatic scandal that Israel only slowly recuperated from over the following year.

Confronted with the growing digital capacities of its opponent, the IDF rapidly built its own; the Spokesperson's Unit was filled with young soldiers adept in social media and some four hundred volunteer students recruited from a private Israeli university supported by the Israeli government and the IDF (Rodley 2014). In Operation Pillar of Defense, an eight-day attack on Gaza, the IDF made use of Twitter and liveblogging to give its up-to-date version of events, running a "hyper-pugnacious" online campaign (Shachtman and Beckhusen 2012). Meanwhile, the Palestinians, with the assistance of Anonymous, mounted major DDoS attacks on Israeli websites. With both protagonists acutely aware of the Twitter revolutions of the previous year's Arab Spring, #IsraelUnderFire confronted #GazaUnderAttack.

When, in 2014, Israel launched the fifty-day Operation Protective Edge against Gaza, with sustained aerial bombardment followed by ground invasion, both sides unleashed what Chris Rodley (2014) terms "viral agitprop" disseminated across "crowded, competitive and fast-moving" social media, with videos, infographics, Twitter feeds, "hypermediated" pop-cultural allusions, "clickbait" headlines, and "meta-commentary" on the antagonist's material. This was aimed not so much at the adversary, for antagonisms were solidified and the messaging was conducted over unshared feeds, but, as Rodley puts it, at "winning support from foreign audiences, rearticulating national identity, boosting morale, and . . . neutralizing enemy messaging." Because viral agitprop is distributed in small, real-time bursts, unlike a feature article or television broadcast, a single channel or user is "able to generate a wide range of material performing a diverse range of functions each day of the war" (Rodley 2014). Militarily, Israel won the war, or at least inflicted by far more casualties than it suffered. Politically, in terms of public opinion and propaganda, the outcome was far from clear cut. Since 2014, networked hostilities have continued; the government of Israel has frequently complained to Facebook about pages allegedly containing Palestinian instigations to violence, and many, including those of politicians, bloggers, and journalists, have been taken down; Palestinians claim Facebook does not respond similarly to complaints about pages in Hebrew inciting violence against them (Greenwald 2017b).

With these two examples in hand, as well as others provided in previous chapters, we can perhaps now say that "this is what cyberwar mobilization, or the militarization of general intellect, or the digital *levée en masse,* looks like," so we now proceed to a more theoretical analysis of this condition.

THE CYBERWAR APPARATUS

In Althusser's discussion of ISAs, the famous example is that of a citizen's spontaneous response to an abrupt "interpellation" or "hailing" by police—"Hey, you!"—immediately self-identifying as an obedient subject to the force of law and order. This instance Althusser takes as paradigmatic of how an array of institutions—schools, churches, political parties, trade unions, media—speak to, summon, name, or address individuals in such a way as to induce an apparently autogenerated compliance with the dominant social order. Althusser wrote before the popular adoption of the internet, so if we return to the notion of ISAs, it must necessarily be as a revision, specifying new interpellative institutions operating through what we will for the moment simply call the *cyberwar apparatus.*

This is an apparatus that emerges at a stage in the development of digital networks very different from that of the electronic frontier or the dot-com boom, when notions of digital autonomy and nomadism flourished. The rise of cyberwar is contemporaneous with the ascent of Google and Facebook in the mid-2000s. Cyberwartime is the time of "Web 2.0" and of the reconceptualization of digital media not as publisher but as "platform," managing proprietorial software that offers tools for structured but self-directed network activities and community creation, the monitoring and measurement of which supplies the big data—generated and collected in astounding "volume, variety and velocity," to use a familiar characterization—that are processed and analyzed algorithmically to target the advertisements that are the major revenue source for the great social media and search engine enterprises (Bratton 2016; Srnicek 2016).

In this context, we see some inadequacies in Althusser's concept of interpellation. For one, his theory of ideology, apparatuses, and subjectification was, from the start, too bluntly state-centric. It asserted that the function of ideology was to secure the reproduction of capital, but did not adequately acknowledge how capital in its corporate form itself undertakes this task, as, in the very processes of commodity circulation, it socializes populations to the relations of production and consumption.[8] This, as the Frankfurt School pointed out long ago, is a process especially assumed by the "culture industry." Today, it has hypertrophied into a cycle of 24/7 entertainment, where, Žižek (1997b) says, we are interpellated by a constant exhortation to "fun" and where the disciplinary functions of ideology are interfused with enjoyment (Flisfeder 2018, 42). This is nowhere more so than in the realm of the digital platforms.

And here we can also see that the Althusserian concept of interpellation is too cognitive; what is missing is the body, the *physical body* of the subjectivized individual that is *colonized* within the information economy of capitalism. Today, not only chatting, liking, sharing, gaming, viewing, and other *fun* has become *work* but also walking, breathing, sleeping, and doing nothing, as these activities are submitted to technological surveillance (Cederström and Fleming 2012). By introducing the notion of the corporeal "speaking being," the *parlêtre,* in his later work, Lacan brings forward the physical body that is speaking and laboring in one joint act.

The body as "the site of discursive production," Tomšič (2015, 20) reminds us, "contains two aspects: the production of subjectivity and production of jouissance," which is as much enjoyable as it is exhausting. Just as labor power becomes a commodity in capitalism, so does *jouissance* in "communicative capitalism" (Dean 2009). A striking example is provided by the case of the company Strava, which, in November 2017, published an interactive map showing fitness-tracking activity around the globe (Sly 2018), thereby inadvertently revealing the running paths of military personnel in war zones where only soldiers are likely to wear fit-bits, outlining a suspected CIA base in Mogadishu, Somalia; a Patriot missile system site in Yemen; U.S. Special Operations centers in the Sahel region of Africa; the main Russian airfields in Syria; and other "undeclared facilities throughout Syria belonging to both Russian and NATO forces" (Sly 2018; Scott-Railton 2018). When the communicating subject, the *parlêtre,* is not only at work but also at war, where it speaks, it enjoys itself to death.

In "platform capitalism" (Srnicek 2016), users validate their existence through an assemblage of social media profiles, postings, preferences, inquiries, recommendations, and all the other digital footprints that represent it within a "programmed sociality" (Bucher 2012a). It occupies "a position [that] never allows someone to enter it fully formed," always rendered "comparable and interchangeable through various qualifications and quantifications of behavior and impact" (Bratton 2016, 252) for the purpose of extracting value and, at the same time, incessantly engaged by the scopic regimes of the personalized web. As Geert Lovink (2016) observes, referencing Althusser via Wendy Chun's (2004) earlier "On Software," the user is "interpellated" by social media from the moment of sign-in:

> Before we enter the social media sphere, everyone first fills out a profile and choses [*sic*] a username and password in order to create an account. Minutes later, you're part of the game and you start sharing, creating, playing, as if it has always been like that. The profile is the a priori part and the profiling and targeted advertising cannot operate without it. The platforms present themselves as self-evident. They just are—facilitating our feature-rich lives. Everyone that counts is there. It is through the gate of the profile that we become its subject.

Or as Ganaele Langlois et al. (2009) put it, "commercial Web 2.0 platforms are attractive because they allow us, as users, to explore and build knowledge and social relations in an intimate, personalized way," while at the same time paradoxically "narrowing down the field of possibilities" in ways that "favor the formation of specific subject positions." This is now the battlefield of cyberwar. In the arena of what is all too aptly dubbed "iWar" (Gertz 2017), the state apparatuses, apparently exceeded and supplanted by corporate forms of ideological address, abruptly reappear, their interpellations lodged in and relayed by the "likes," "tweets," "recommendations," and "follows" at the very heart of digital sociality and identity formation.

A state's interpellation of its subjects, or of the subjects of another state, is in part a question of its cyberwar apparatuses' access to or interdiction from specific platforms. Though platforms may be more or less global or local in scope, they are also national, in terms of ownership and legal governance and relations to a homeland state security apparatus. This is a dynamic around which the profit interests of specific blocs of digital capital and political interests of security state apparatuses mutually revolve (Google / Facebook / Twitter for the United States; VKontakte / Yandex for Russia; Weibo / Baidu / Tencent for China). "National" interpellation of state subjects is manifestly in play in the banning by the Ukraine government of Russian social media and search engines in the midst of an ongoing war. It may also, however, manifest when military conflict is merely anticipated, as we saw in chapter 1 in regard to the "Sino-Google war" (Bratton 2016, 112) and its imbrication in intensifying China–United States hostilities.

However, cyberwar subjectification is not simply a question of demarcating "national" platforms and "national" identities. The profit dynamics of Web 2.0 capital demand both an ever-enlarging user base and the self-activity (and hence self-revelation) of users. Because of this, it is possible to construct within social media interpellative micromachines, that is to say, specific user communities, as a sort of "partisan" presence inside ostensibly foreign digital territory. Within Facebook, one can form a nation, or a caliphate, or perhaps even an assembly or commune. Platforms owned by capital of another state, even an adversary state, can be seeded with subversive practices or used as digital territories across which wars are fought between other competing states, as the Gaza conflict was digitally fought out across Twitter. The truly global social media platforms, owned by U.S. capital, are particularly liable to this process, precisely to the degree that their huge profitability depends on amassing global users. This cyberwar seeding of subjectification involves agents. These are of various kinds: state military public relations agencies, such as the IDF's Spokesperson's Unit (now being widely copied by other militaries); clandestine troll armies, such as those of Russia's Internet Research Agency; U.S. military "sock puppets"; or ISIS militant recruiters. The efforts of such agents may also be articulated with autonomous interpellative processes, such as those of dissenting movements within foreign states or citizen journalists with a spontaneous patriotism for the homeland. Agents may work positively, as "friends"; negatively, harassing enemies; or in contradictory, chaotic directions, generating a paralyzing anomic blur. Each of these comes with its own interpellative processes.

For example, one can contrast the careful cultivation of the subject of an ISIS recruitment process with trolling practices associated with Russian hybrid warfare. In the former process, recruiters "monitor online communities where they believe they can find receptive individuals," sifting through visitors to militant sites. They then create a warm virtual microcommunity around potential recruits, saturating them with messages that, depending on the orientation of the target, may emphasize religious devotion, the appeal of violent action, grievances against racism, religious discrimination, poor economic prospects, or positive depictions of life in militant-held territories. At the same time, they encourage the potential recruit to isolate himself from other contacts. At a certain point, communication shifts from public forums into private and encrypted channels. It is in this phase that options such as emigration to ISIS territory, as a civilian or fighter, or attacks at home are discussed. The cycle is a sustained, modulated "hailing" of an identified data subject as a supporter of the caliphate, a data relation that then translates into corporeal action (Berger 2015a, 2015b).[9]

Cyberwar trolling is an interpellation that reverses the logic of recruiting. An enemy, rather than a friend, is identified, vilified, enraged, exhausted, and metaphorically (and sometimes literally, through "doxing" and the like) destroyed, silenced, intimidated, or forced offline—with the correct subject position established negatively, in contrast to that of the unfortunate and despicable victim. While the term is loosely applied to many forms of online harassment, it is often more specifically used to characterize a strategy of escalating rancorous dissensus, for example, making a provocation that can be bootstrapped into intensifying abuse and insult. In this form, trolling is sometimes analyzed as having a distinct sequence; the lure, the catch, reeling in, and so on. It may be practiced solo or in teams (with one troll reinforcing another or making an apparently innocent conversational setup that can later be exploited) and can involve a number of gambits (such as professing support for a position but then undercutting it with damning "concerns"). Thus, for example, on a nationalist Ukraine internet forum, pro-Russian trolling can ramp up from an apparently measured remark about U.S. support for Ukraine to intensifying attacks on Ukraine's corrupt incapacity for self-governance, Western homosexual degeneracy, ubiquitous fascism, cowardice, and inevitable defeat. The subjectifying address is "if you are like that, you are worthless; you don't want to be like them, the faggots/fascists/CIA dupes, but like us, your brave Slavic brothers" (Szwed 2016).

Though cyberwar apparatuses require agents, they depend on virality (Sampson 2012). A first, minimal sign of a successful digital interpellation is that it generates a "like," a "retweet," a "follow." It is in the nature of the viral process that it becomes difficult to distinguish instigators from followers; it aims at user complicity.[10] Such virality is not just a communication of discursive political positions and arguments. It is a "transmission of affect" (Brennan 2004), a process of emotive contagion. This is why images, particularly images of the horrors and atrocities of war, variously authentic and fabricated, are so important. The IDF uploads video from the helmet-mounted camera of an Israeli soldier in urban combat in Gaza; the fifteen-year-old girl Farrah Baker, one of the most effective of Palestinian citizen journalists, tweets a photo of the night sky above her home blazing with flares in the midst of intense aerial bombardment, accompanied with, "This is in my area. I can't stop crying. I might die tonight #Gaza #GazaUnderAttack #ICC4Israel [International Criminal

Court for Israel]" (Patrikarakos 2017, 30). Both interpellate by eliciting identification with a moment of intense affect—the excitement of combat, the fear of death—that entrains a political sympathy.

There is no guarantee of virality (unless it is artificially boosted by bots); any given interpellation may be wasted, washed away, interrupted, contradicted, and cancelled or co-opted in the babel of social media voices and vanish without a trace. Conversely, various interpellative sequences, with or without common origin, may start to resonate with one another. As we have already suggested, the importance of the clandestine advertisements of the Internet Research Agency around the 2016 U.S. presidential election, with their invocations of threatening immigration, dangerous minorities, Clintonite Satanism, and diffuse but intensified social antagonism, was only as one element in a digital surround-sound interpellation of the U.S. electorate conducted simultaneously from multiple directions—the official Trump campaign, the alt-right's autonomous digital networks, Macedonian for-profit web news producers—that together generated multiplying addresses constructing an aggrieved, white, American–patriotic subject under attack from people of color, Islamic terrorists, political elites, foreign job stealers, and miasmic social anomie. Such compounding and escalating interpellations generate waves of viral affect (Massumi 2015), increasing the probabilities of summoning up a respondent to the proffered subject position.

In 2011, Eli Pariser brought to public attention the phenomenon of "filter bubbles." Since then, the concept has been used to criticize the personalized web for producing a pacifying sense of self-conformity. However, subsequently, we have seen the growing antagonisms within or between these echo chambers. Such antagonisms are exploited by state or insurgent powers that build on the preliminary work of automated segregation performed by commercial algorithms generating consumer profiles. Peter Sloterdijk's (2011) "spheric project" of bubbles, spheres, and foams helps conceptualize these network productions. Between the microspheric bubbles of the intimate and the macrospheric globes of a historicopolitical world lie the "foam worlds" of Amazon, Google, Facebook, Twitter, Weibo, and VKontakte, where "the individual bubbles are not absorbed into a single, integrative hyper-orb . . . , but rather drawn together to form irregular hills," making "what is currently confusedly proclaimed *the* globalization of the world [a] universalized war of foams" (71). This for Sloterdijk is "the modern catastrophe of the round world" (70): the "spheric blasphemy" (69) of antagonized plurality.

In turn, interpellative networked interventions by antagonists spur states to the adoption of homeland censorship and/or surveillance systems, with the aim of blocking or deleting hostile virality and detecting or eliminating its instigating agents. The two elements in this censorship–surveillance ensemble are distinct but related. Censorship implies a monitoring and disciplining of those who attempt to evade it, and surveillance, if known or suspected, results in the internalized discipline of self-censorship. What is in play here, however, is, as John Cheney-Lippold (2017, 169–72) points out, not so much a state's direct address of the subject as its observation and categorization of that same subject, be it as a "good citizen" or "terrorist suspect" or "foreign agent." This disturbs the "clean cut" (Dolar 1993) finality and determinism of Althusser's model of interpellation. It posits a subject that is not talked *to* but talked *about*—a subject of surveillance not usually aware of the identity bestowed on it but that, suspecting surveillance, does its best to avoid suspicion. This subject is not immediately exposed to the "hey you" hail of the police but may become aware of her "composite algorithmic identity" from the changing nature of interpellations, say, at a routine traffic stop, by a guard at a border crossing, or during an airline passport check (Cheney-Lippold 2017, 170).

Panoptic surveillance and virtual mobilization are reciprocally related in complex and contradictory ways. It is the potential for subversive mobilizations that evokes state surveillance, yet states also increasingly themselves mobilize virtual recruiters, troll armies, patriotic hackers, and social media communities against their opponents. This double face of interpellative incitement and surveillant suppression constitutes a feedback loop constantly reinforcing the cyberwar apparatus. This again revises the Althusserian account of subjectification. For with war, we have a *contest* of interpellations, and a subject played upon by and constituted in that collision, a subject not only addressed by the homeland ISAs but also exposed to adversary address and, because of this, then subjected to processes of surveillance and censorship, watching and blocking, that in turn become constitutive of subjectivity.[11]

Because cyberwar interpellations largely depend on for-profit social media platforms, they, at root and regardless of source, reinforce the interpellation of the "user" as a subject of global digital capital. But this interpellation is also and simultaneously the constitution of the subject of particular fractions and blocs of digital capital, aligned against one another in association with antagonistic national security states and would-be states. The interpellative process is thus split by the inescapable contradiction between the one, total capital of a planetary system and the many, competitive, hostile capitals composing that totality. In cyberwar, this agonistic process of interpellation, conducted in the fast flows of social media, intensifies the always unfinished and ineradicably incomplete nature of subjectification, an element of Lacan's thought that Althusser arguably misunderstood or abandoned in his original account of the ISAs.

In summary, cyberwar operates through apparatuses of subjectification that work across platforms and are aimed at the populations of these platforms (populations that can be conceived of as combined human–device assemblages) both at home and abroad. This apparatus employs specific agents (bearing in mind that, as we will discuss later, these agents may be wholly or partially automated) that issue the interpellative call or summons (itself the outcome of long-preceding chains of interpellative subjection). But this call thenceforward depends for its efficacy on networked contagion (whereby if the process "takes," each interpellated subject becomes an interpellator), a process that may go nowhere but whose accumulative outcome can be filter bubbles or echo chambers (the death stars or black holes of cyberwar) of autodisciplining subjects. The preemption and targeting of such digital enemy partisans, real or imagined, become the task of the conjoined surveillance and censorship mechanisms by which each regime's cyberwar apparatus attempts to prevent its own infiltration and disrupt the adversary. This is how cyberwar engages the continuous process of reproducing the "economic, political, juridical and cognitive fiction of the subject" (Tomšič 2015, 6).

Just as Althusser suggested that the ISAs comprised a range of institutions—school, church, media—each of which operated in its own particular register and could be variously articulated with the others, so cyberwar apparatuses are a collocation of institutions and practices—soft power, digital propaganda, troll armies, internet recruiters, surveillance and censorship—that can be variably permutated with one another by any particular state or quasi-state. The old ISAs do not disappear (positing such a world remade *ab novo* by digital networks would be the worst version of ideology) but rather collaborate with, are reshaped and reinforced by, the cyberwar apparatus. Thus, for example, Zeynep Tufekci (2017) notes how under Turkey's authoritarian Erdoğan regime, engaged in the double repression of domestic dissent and war against Kurdish rebellion, a major governmental strategy has been to *discourage* the populace from using social media, widely used by regime critics, disparaging it as a realm of perversion and deceit, aiming instead to retain the people within the orbit of television watching, where the state feels more secure in its control of content.

We are in a zone where "algorithmic ideology" (Mager 2012), "algorithmic governance" (Just and Latzer 2017), or even an "Algorithmic Ideological Apparatus" (Flisfeder 2018) meets with "algorithmic war" (Amoore 2009). However, we do not speak only of ideological effects. Althusser's (1971) original formulation divides the "ideological state apparatus" from the "repressive apparatus," comprising the military and security forces, and emphasizes that, while each has both ideological and repressive components, the former operates "massively and predominantly" by ideology, the latter primarily by violence (145).[12] In the case of cyberwar, we argue that the weaponization of communication means there is a cross-over between the ideological and violent operations; while some activities, such as computational propaganda, fall on one side of the spectrum, and others, for example, a nuclear facility–destroying computer worm, fall on the other, there is an intermediate zone where so-called social engineering and viral propagation are indispensable to both. Althusser reminds us that "there is no such thing as a purely repressive apparatus," because "even though the Ideological State Apparatuses function massively and predominantly by ideology," "they also function secondarily by repression" (145). On the global scale, these two systems of control, one forcing users to speak and another silencing them, are inseparable, like two sides of a Moebius strip, despite the illusionary division, constitute one surface. It becomes almost impossible to determine where the bigger danger rests. But it is already clear today that everything said—and, even more so, the unsaid—will be held against us tomorrow.

SEXING CYBERWAR

The subject of cyberwar, like the subjects of all wars and like the subject in general, is sexed. This is implicit in all the historical analogies we have invoked; the nomad warriors are men, the *levée en masse* is universal *male* conscription. In this section, we draw on the rapidly growing literature of feminist security studies (Åhäll 2015; Brunner 2013; Enloe 2016; Sjoberg 2014) to consider three hypotheses about the gendering of the cyberwar subject. One emphasizes the exclusion, subordination, and victimization of women in cyberwar. Another, in contradiction, speaks of the emancipatory possibilities such war opens for them. Lacan's views on the matter of sexed subjects significantly differ from these two positions. For him, "sexuation" is not related to biological sexuality and gender; instead, Lacan (1999) describes "masculine" and "feminine" ontologically, as symbolic positions that the subject assumes in relation to the laws of universalization. Thus the Lacanian question is whether the subject can escape the universal law, here that of cyberwar and its totalization. "Masculine" logic is the logic of grouping with the same, driven not by the sense of solidarity but rather by growing insecurity toward others, which immediately mobilizes the need to exclude the uncomfortable encounters. "The feminine" position is not clearly defined: these data subjects are resistant to accept their imposed data identity as a solid, recognizable, readable, stable spatial and temporal data pattern. Instead, they investigate their data representation as, always, a misrepresentation, an inconsistency in data identity. These data subjects, no matter their sex and gender, are not (or are not fully) the subjects of the "universal" laws of cyberwar. From this perspective, we find more promise in a third perspective that takes up the issue of the sexed subjects of cyberwar in the broader context of the relation of information warfare to neoliberal capitalism.

In many ways, cyberwar interpellates women as subjects of exclusion and victimization. It hyphenates two domains, cybernetics (or more broadly computing science) and war, that have both traditionally been culturally coded as male (Hicks 2018). This is so despite the fact that women were present at the origins of cyberwar. Female "computers" programmed the ENIAC, the mainframe machine used in the design of the atomic bomb (Abbate 2003). About eight thousand women worked in Bletchley Park, the site of the British "Enigma" program of computerized cryptoanalysts during World War II, operating cryptographic and communications machinery, translating documents, and performing traffic analysis and clerical duties (Burman 2013). Also during the Second World War, a majority of NSA cryptoanalysis personnel were women (Budiansky 2016; Mundy 2017).

However, this female presence at the origin of cyberwar was subject to a triple erasure. First, the overall masculine path of military–technoscientific development ensured women working on early computer projects were mostly subordinated to, and hence eclipsed by, men. Second, most were at the end of the war rapidly replaced either by men or by computers overseen by men. Third, their contribution was then largely forgotten, in one of the "invisibilizing moves" by which women have repeatedly been "written out of the histories of war" (Sjoberg 2014, 148). Both the military origins of cybernetics and the forgetting of women's part in those origins became part of a series of self-reinforcing cultural feedback loops that constructed computing science as a predominantly and "naturally" male discipline. This has in turn ensured that the central, or at least most prominent, subjects of cyberwar, hackers, are predominantly male.

This gendered construction of computing science would in the United States and Europe from the 1970s onward be challenged by successive waves of feminist technoactivism and advocacy, which, for a time, seemed to make some ground. Donna Haraway's famous call in 1984 for a "cyborg" socialist feminism that would make digitalization "unfaithful" to its military–industrial origins named this this apparently rising trend. It is therefore ironic that from the time of the publication of "Cyborg Manifesto" in the mid-1980s, women's enrollment in U.S. computing programs began a long decline from which it has not recovered. Paradoxically, the cause for this may lie in the expanding popular use of personal computers, which entered households under the auspices of corporate marketing campaigns targeting them to men and boys and linked with an initially highly militarized and masculinized video game culture that gave young men an intense head start in all things digital, independent of formal schooling (Kline, Dyer-Witheford, and de Peuter 2003).

Today computing science, and cybersecurity in particular, remain male professional fortresses.[13] This is the case even while women are, in many parts of the world, highly active in social media and other aspects of networked communication. It is therefore possible to present the gendering of cyberwar as a process in which the digital domains of a femininity acculturated to civilian conversation are turned into battlefields and devastated by high-technology militarized masculinity. This analysis can be supported by pointing out that not only the participants in cyberwar but some of its characteristic practices are gendered. For example, "trolling" is characteristic of misogynist and homophobic digital discourse; there is a manifest overlap between the rise of cyberwar and surging toxic masculinity on Twitter and other social media, sometimes termed "the cyberwar on women" (Thistlethwaite 2016). In the Syrian civil war, female human rights activists using social media in protesting atrocities and documenting the use of rape as a weapon are at risk from government online surveillance and from the hacking of pro-Assad digital militias, such as the Syrian Electronic Army, gathering personal information that puts their lives in danger and "wreaking havoc in online spaces" (Radloff 2012). In this aspect, the cyberwar apparatus's interpellation of its subjects recapitulates in a new technological register the classic binary of male soldiers and female civilians, violent masculinity and pacific femininity, violating men and violated women.

But cyberwar also has a countertendency to hail women as important, even indispensable, protagonists. If social media are a battlefield, trolling is only one of the tactics deployed on it. Others, including viral appeals against enemy atrocities or for defense of the homeland or various forms of "psychological operations," mobilize sentiments and aptitudes associated with traditionally female subject positions attuned to interpersonal and affective interactions. In the Syrian civil war, between

2013 and 2014, a pro-government hacking group operated a scheme by which a female avatar would contact male rebel officers and opposition members on Skype, strike up a conversation, and share a "personal" photo with them; "before sending the photo she typically asked which device the victim was using—an Android phone or a computer—likely in an effort to send appropriately tailored malware" (Reglado, Villeneuve, and Scott-Railton 2015). Once the target downloaded the malware-laden photo, the hacking group accessed his device, "rifled through files and selected and stole data identifying opposition members, their Skype chat logs and contacts, and scores of documents that shed valuable insight into military operations" (Reglado, Villeneuve, and Scott-Railton 2015). Who was behind the "female" avatar is uncertain, but "she" spoke from one of the stereotypical positions assigned to women in war, that of the femme fatale seductress-spy. Other examples are less ambiguous and more innovative. We have already referred to the important role played by female bloggers in Gaza in galvanizing international outrage at Israeli air bombardment. Many of the Israeli military personnel countering their efforts were also women; the IDF's Spokesperson's Unit reportedly had a high proportion of young female soldiers in its ranks, who senior officers considered especially adept at fighting a war for networked public opinion (Patrikarakos 2017).

In her study of "sexing war," Linda Åhäll (2015) addresses the increasing recruitment of women by militaries around the world. She suggests that war waged across networks is one of a number of factors reducing the importance of "brute strength" in soldiering and blurring lines between peace and war. This means that "exclusion policies keeping women out of certain positions within the armed forces have become more and more difficult to justify and . . . more and more positions open up to women" (3). She cites as an example the opening to women of combat roles in the armed forces of the United States and other countries, but the process is also marked in cyberoperations, where it may even be breaching the divide that has segregated women into social media roles and men into programming positions.

One of the very few specific studies of gender in cyberwar, by Alexandria King-Close (2016), argues that U.S. Cyber Command and other branches of the Pentagon have in recent years made strong efforts to recruit women to cyberoperations. About one-third of its employees, and more than one-quarter of its "professional computing" jobs, are held by women, a proportion higher than the overall percentage of women working in information technology roles in the United States (King-Close 2016, 38). In the United States, recruitment of hackers by the state has now become a national security problem, because they can get higher wages in the corporate sector (Slaughter and Weingarten 2016). The Pentagon is taking emergency measures. One is the increased use of privatized contractors (which brings with it its own security problems). Another is recruiting women. In 2015, Theresa Grafenstine, the inspector general of the U.S. House of Representatives, spoke to the issue: "We are absolutely in the middle of a cyberwar," she told a congressional briefing. "It's a new cold war." Presenting data demonstrating that America's cybersecurity workforce is dominated by men, she declared, "If you think we're going to win this war with only half our army—they're going to eat our lunch!" and robustly suggested it was time to "slap Cinderella with a laptop" (Bratton 2015). Thus Haraway's "cyborg" feminism is now exhorted to recover its faith in the military–industrial complex.

In this context, where enlistment as a cyberwarrior is promoted as a feminist path to computational gender equity, the complex work of Elgin Brunner (2013) on the interaction of gender, military institutions, and neoliberalism is especially important. She analyzes the gender assumptions embedded in the discourse and practice of "information war," "perception management," and psychological warfare operations by the U.S. Army in Iraq, operations that now would be considered to fall squarely in the zone of computational propaganda. Her argument is that, regardless of the personnel carrying it out, information warfare's premises are gendered, insofar as they "recur to the most basic stereotypes about what masculinity and femininity imply, namely the holding of and subordination to power," whereby "the Self is hegemonically masculinized and the Other is feminized" (106), with the "capacity to influence . . . among the active and shaping qualities associated with masculine power and skill" and the "quality of being influenced has a negative connotation . . . associated with feminine subordination" (106). In military terms, to be one of "us" is to be automatically masculinized vis-à-vis an enemy who is always, structurally "feminized."

Brunner's (2013) argument is thus that military institutions are so deeply and historically sexed in their conceptions of power that they are "masculinized" regardless of the gender of concrete participants. War is a "gendered identity performance of statehood" (8), a mustering of subjects under the sign of a masculine homogeneity. In this sense, the military is an institution of "hegemonic masculinity"—"structured not only by the hegemony of masculinity over femininity, but also by the domination of one masculinity over other masculinities"—and in that regard it "has not changed since the integration of women" (24). The new emphasis in cyberwarfare on networked organization, flexibility, technological competence, and speed, which in some wars open the fields of "psyops" and "information warfare" to women, only modulates this deeply sedimented structure. This shift Brunner sees as congruent with the rise of neoliberalism, in which the celebration of the network-connected free market hides a subtext of rampant interstate antagonism, such that military information warfare overlaps with economic competition. Her analysis thus joins that of other feminists who point to the very specific shaping and limitations of gender-equity initiatives, and the push for diversity and inclusion, in the context of neoliberalism and militarization (Fraser 2013; Enloe 2016).

Much of the analysis of the gendering of cyberwar addresses its U.S. iterations: there is little or none available in English on the place of women in Russian, Chinese, Iranian, or other cyberwar apparatuses, where their presence may take quite distinctive inflections. Acknowledging this as a void in our understanding of cyberwar subjectification, we now want to take another direction. For if, as Brunner (2013, 104–6) argues, the drive for "technological omnipotence" is a deep dynamic of masculinization, militarization, and neoliberalism, this raises the possibility that the human participants in cyberwar, however gendered, may be overtaken by the intensifying production of automated cyberwar assemblages.

AUTOMATIC SUBJECT

We have argued that cyberwar entails a mobilization of networked subjects, a digital *levée en masse* or militarized "general intellect." This is, however, a paradoxical process because of its relation to automation. Historically, the total war enabled by mass conscription became an ever more mechanized war; in capital, the "general intellect" is activated to automate production, including ultimately its own production, creating a system in which, while human presence remains, it is only as a "link" between machinic components (Marx 1973, 691, 693). Cyberwar, at the cutting edge of a highly automated phase of capital, is fundamentally a process of machinic mobilization, in which humans increasingly play the role of relays within processes whose speed and complexity are deeply inhuman, or at least ahuman. The subjects of cyberwar are thus ultimately not so much humans as they are machine networks to which humans are the most easily compromised point of access. There are several faces to this: the deployment of bots in computational propaganda; the ever-intensifying automation of swarming DDoS attacks; the deployment of massive criminal/military botnets; and the application of advanced forms of artificial intelligence to cyberwar attack and defense.

A chatbot (aka bot, interactive agent, or artificial conversational entity) is a computer program that, through speech or text, converses online. While some bots, such as Apple's Siri or Amazon's Alexa, are overtly machinic, others, often encountered online in Twitter feeds or chat rooms, masquerade as human. Their capabilities range from simply retweeting messages or following a purportedly popular account or mobbing a selected target to convincingly simulating a human interlocutor. They can be preprogrammed with a limited repertoire of conversational gambits, but advanced forms learn from their networked environment. In the infamous case of Tay, a Microsoft chatbot meant to emulate the conversation of a teenage girl, exposure to U.S. internet exchanges resulted in prompt acquisition of misogynist, anti-Semitic, and racist conversational tropes. Some social media companies not only permit bots but tacitly encourage them by making automation easy, as they build traffic volume and create the appearance of vibrant activity, which is good for market valuation.

Twitter has made itself especially bot-friendly; recent estimates suggest that as much as 50 percent of its traffic is automated (Gorwa 2017).

The ubiquity of chatbots means much cyberwar interpellation is performed by machinic agents that can, at least temporarily, pass the Turing test. Bots are generally believed to play a significant role in computational propaganda campaigns emanating from Russia, such as those directed at Estonia in 2007, Georgia in 2008, and Ukraine from 2014 onward. Twitter has identified more than fifty thousand accounts that were engaged in "automated, election-related activity originating out of Russia" during the 2016 U.S. presidential race (Machkovech 2018). These are far from the only examples. In 2017, a political crisis in the Persian Gulf area saw Saudi Arabia and the United Arab Republic accuse Qatar of sympathy with Iranian-supported terrorism and insurgencies. Qatar claimed this was a smear campaign. According to an analysis by *Washington Post* journalist Marc Jones (2017), 20 percent of the active anti-Qatar Twitter accounts were bots, "posting well-produced images condemning Qatar's relations with Hamas, Iran and the Muslim Brotherhood." The bots also "singled out Qatar's media channels as sources of misinformation," tweeted support for the Saudi monarchy, and, during the Riyadh United States–Saudi Arabia summit, "posted thousands of tweets welcoming Trump to Saudi Arabia." Jones (2017) comments that this "mobilization of Twitter bot armies," rather than conveying "an organic outpouring of genuine public anger at Qatar," showed that "an institution or organization with substantial resources has a vested interest in popularizing their criticism of Qatar."

A higher level of cyberwar automation is the DoS attack, in which the perpetrator tries to make a network resource, for example, a website or email service, unavailable by flooding the target with messages. In a DDoS attack, the incoming messages come from many different sources, making the assault harder to counter. DDoS attacks are weaponized machinic interpellation, "hailing" the target so many times that it malfunctions in attempting to reply. From their origin, DDoS attacks have involved software tools for scheduling and sending repeated messages to the target. However, these tools were often used manually, by a single user seated at his own computer, so that successful attacks required large numbers of active human participants. In this form, DDoS could be (and by some still are) seen as a mode of digital insurgency against state and corporate power: examples include DDoS attacks made by the group Electronic Disturbance Theatre from 1998 to 1999 in support of the Zapatistas, using the FloodNet program, and Anonymous's Operation Payback and Operation Avenge Assange a decade later, attacking the sites of corporations attempting to shut down radical organizations, such as the Pirate Bay and WikiLeaks, with its Low Orbital Ion Cannon DDoS tool (Sauter 2014, 109–35; Deseriis 2017).

Such attacks have, however, rapidly entered the repertoire of state power. Britain's Government Communication Headquarters (GCHQ) reportedly retaliated against Anonymous with a series of DoS attacks against its servers in what it called Operation Rolling Thunder (Sauter 2014, 146). DDoS operations are now a common feature of interstate cyberwar, using increasingly automated tools. Evgeny Morozov (2008) narrates how he "signed up" to become a "soldier" in what are widely believed to be Russian-sponsored DDoS attacks on websites in Georgia during the 2008 war between the two nations. This enlistment, far from involving hacker expertise, involved only surveying "the Russian blogosphere," getting directions to a designated website, downloading some easy-to-use software, and, from a pull-down menu, selecting targets—"the Ministry of Transportation or the Supreme Court?"—and clicking "Start Flood." One of Morozov's points is that his experience undermines the assumption that DDoS attacks coming from Russia are necessarily performed by highly trained state operatives; the process is easy for "patriotic hackers" with relatively low digital literacy to undertake, whether spontaneously or through arm's-length state orchestration. In this form, DDoS attacks can be considered a classic instance of the digital *levée en mass*. But what makes this feasible is automation: "war at the touch of a button" (Morozov 2008).

The swarm logic of the DDoS attacks is preserved but raised to a higher level in botnets (from "robot" and "network"), networks of computers (servers, desktops, laptops, smartphones) penetrated by malware so their operations can be controlled by a third party as "zombie armies." Botnets have existed for decades, controlling devices in numbers from the tens and hundreds of thousands to millions. The "botmaster" has at her disposal huge amounts of computing power and bandwidth that can be directed not just to execute DDoS attacks but also to steal data or implant malware. Sometimes participants volunteer to have their computers infected: Anonymous used a type of botnet in the operation of its Low Orbital Ion Cannon, and so did the student group Help Israel Win, which attacked pro-Palestinian websites during the 2009 Gaza War (Shachtman 2009). But users usually do not realize their devices have been compromised. There is a thriving dark web market for purchase or rental of off-the-shelf botnets running on the computers of unknowing participants (Keizer 2010). In such systems, the human is recruited by a phishing attack that will open new networks to viral infection, enlisted only as a vector for access to machinic power.

Botnet capacities are now amplified by the advent of the Internet of Things (IoT), that is, the embedding of networked digital sensors in industrial infrastructures, surveillance cameras, thermostats, baby monitors, televisions, and refrigerators that can communicate with one another, all of which can be used as botnet components. In 2016, the Mirai botnet, drawing on the digital "firepower" of such devices, launched some of the most disruptive DDoS attacks ever known, temporarily shutting down Dyn, a company important in directing internet traffic, and largely knocking the country of Liberia offline. Other "IoT cannons" are almost certainly being produced (Krebs 2016). While to date, botnets such as Mirai are principally used for criminal purposes, the membrane between crime and war is (as we discuss in the next chapter) highly permeable. It is thus almost certain botnets already have a place in military cyberarsenals.

In 2017, the U.S. government's Computer Emergency Readiness Team (2017) issued a warning that North Korean cyberwar plans (given the orientalist code name Hidden Cobra) included a DDoS botnet infrastructure, Deep Charlie, described as "capable of downloading executables, changing its own configuration, updating its own binaries, terminating its own processes, and activating and terminating denial-of-service attacks." In other words, it was a highly automated, semiautonomous system. While such reports can be suspected of recapitulating the notorious "weapons of mass destruction" alarms that preceded a U.S. attack on Iraq, they are not completely implausible. The alert was issued in a context where U.S.

cyberattacks on North Korean intelligence agencies were reported to proceed "by barraging their computer servers with traffic that choked off Internet access" (DeYoung, Nakashima, and Rauhala 2017), so "stack versus stack" (Bratton 2016) hostilities between the two nations may include covert botnet wars.

A striking example of the automated power wielded by nation-state cyberwar apparatuses was the appearance in 2015 of China's Great Cannon, a programming exploit that redirected internet traffic intended for Chinese websites and used it to flood the servers of websites critical of China's internet censorship policies and hosting censorship-evading tools. Not a botnet but a "man in the middle operation," in which the attacker secretly intervenes in communication between two parties, the Cannon hijacked the communications of unknowing bystanders to give the Great Firewall system of censorship and monitoring a massive offensive capacity (Goodin 2015). DDoS attacks, once the weapons of nomadic and anonymous digital rebels, are now, with massively enhanced automation, part of the arsenal with which states quell and punish such revolts. U.S. and British intelligence agencies have developed capacities to redirect internet traffic similar to those of the Great Cannon, not necessarily for DDoS attacks but as a surveillance method, diverting messages to secret servers that impersonate the websites the targets intended to visit (Weaver 2013).

These examples, are, however, dwarfed by the prospects opened by deployment of new forms of artificial intelligence (AI), such as machine learning, for cyberwar. In 2014, Edward Snowden said in an interview that when he quit the NSA, it was working on a cyberdefense system named MonsterMind that would "autonomously neutralize foreign cyberattacks against the US" (Zetter 2014b). It would operate through algorithms capable of rapidly analyzing huge databanks recording internet traffic patterns, differentiating normal flows from anomalous or malicious activity and instantaneously blocking a foreign threat. Snowden expressed anxieties not only over the scale of traffic monitoring required but also because automated responses might extend beyond defense to retaliatory "hackback" strikes against an attacker. Little more has been heard of MonsterMind and how far, if at all, the NSA advanced with the project. Nonetheless, its described modus operandi is consistent with mounting interest by cybersecurity experts in using machine learning and other forms of AI to detect and respond to unusual computer events that might indicate an attack, rather than relying on the static defense of preprogrammed firewalls (Ward 2017; Rosenberg 2017). This interest is itself a response to the perceived capacity AI gives attackers to rehearse exploits and accelerate the speed of intrusions (Yonah 2018).

As early as 2012, a cybersecurity firm study suggested that more than 51 percent of internet traffic was nonhuman; it claimed that of this traffic, more than 30 percent was "malicious," involving activities such as "'spies' collecting competitive intelligence" and "automated hacking tools seeking out vulnerabilities" (van Mensvoort 2012).[14] Other studies push the date machine-to-machine communication predominates further off—but only into the imminent future (Dolcourt 2017). Therefore, doing some violence to Althusser's interpellation, we can say that much of the "hailing" of subjects conducted by the cyberwar apparatus is performed, not just between machines and human subjects—as with chatbots—but between machines and machines. The IoT comprises devices talking to devices. These Things can be made to act as Weapons; the IoT is also a Web of Weapons. There is today widespread discussion of "autonomous weapons" and the tendency to take humans "out of the loop" of automated war-fighting systems (Singer 2009; Scharre 2018). While missile-firing drones and armed robots are dramatic examples of this drift, invisible processes of cyberwar may be its forward edge. Capital develops its most advanced technologies in warfare; in cyberwar, we see it advance toward a concrete actualization as what Marx (1977, 255) called an "automatic subject" or what Liu (2010) terms the "Freudian robot."

UNCONSCIOUS WAR

Within cyberwar apparatuses, humans, for the moment, remain a necessary link or relay enlisted in multiple ways, voluntary and involuntary. Yet while humans remain in the loop, or on the loop (that is to say, with a veto on otherwise automatic processes), it is within a war-fighting system that increasingly decenters subjectivity as a "peripheral" (Gibson 2015). Because of this, the human subject of cyberwar is dazed and confused.

This is in part a consequence of the intentional secrecy of cyberwar, but the possibilities of such stealth, and its intensification by contingency and accident, arise from the speed, scope, and complexity of the technology of cyberwar apparatuses.

Deeply implicated as users are in the militarization of networks, their involvement is frequently unknowing or misrecognized. We are indeed "empowered" by technology—but not necessarily in the way we are told. Rather than acting as globally aware networked individuals, intervening purposefully in great political events with a few deft touches to an iPhone, our cyberwar involvement is as likely to be a misapprehending, deceived, or involuntary conduit for war whose outbreak has either passed by unnoticed or was only imagined (at least until this imagined onset provoked real counteraction), or whose combatants are drastically misidentified. In conflicts where a crucial action may be the opening of virally contaminated email, the retweeting of a message from a software agent mistaken for a human, or the invisible contribution of a hijacked computer (or digitalized refrigerator) to a massive botnet, we are in the realm of Marx's "they do it, but they do not know it." "Even if you do not see the war, the war sees you" is the logic of the blind gaze of cyberwar, a regime in which although "the subject does not see where [this regime] is leading, he follows" (Lacan 1998, 75).

The obscurity inherent to cyberwar afflicts even those most expert in its prosecution. During the U.S. occupation of Iraq, the CIA and Saudi Arabia's intelligence service set up a "fake" jihadi website to monitor Islamic extremist activity. In 2008, the U.S. Army and the NSA concluded that the "fake" site was actually serving as an operational planning hub for attacks by Saudi Arabian jihadists joining the Sunni insurgency. When they proposed the site be destroyed, the CIA objected, but Pentagon hackers proceeded with the "take-down." They inadvertently disrupted more than three hundred servers in Saudi Arabia, Germany, and Texas. As a task force participant ruefully explained, "to take down a Web site that is up in Country X, because the cyber-world knows no boundaries, you may end up taking out a server that is located in Country Y." The Saudi Arabian intelligence service, which regarded the "fake" site as a "boon," was furious; mollification required "a lot of bowing and scraping." The

CIA, too, was resentful; the agency "understood that intelligence would be lost, and it was; that relationships with cooperating intelligence services would be damaged, and they were; and that the terrorists would migrate to other sites, and they did" (Nakashima 2010).

A more serious example of unintended consequences is Stuxnet, the computer worm planted in the computers at the uranium enrichment plant outside Natanz to prevent Iran from building a nuclear bomb, an operation now widely attributed to a joint U.S.–Israeli intelligence operation. As we noted in chapter 1, the worm's impeccable simulation of a mechanical failure apparently unrelated to software performance is considered a watershed in the development of cyberweaponry. What it is not so generally recognized, however, is that it went out of control. Stuxnet's discovery by the security company VirusBlokAda in mid-June 2010 was the result of the virus accidentally spreading beyond its intended target due to a programming error introduced in an update. This allowed the worm to enter into an engineer's computer connected to the centrifuges and thence travel to the internet. It then propagated to industrial sites far from Natanz, not only in Iran but in Indonesia and India, and beyond, reportedly infecting the systems of oil giant Chevron and a Russian nuclear plant. As one cybersecurity expert puts it, "By allowing Stuxnet to spread globally, its authors committed collateral damage worldwide" (Schneier 2010). Although in many of these cases, the virus did not activate, because of differences between the Natanz system it targeted and the others it accidentally infected, another consequence was that the Stuxnet code became widely available for use or adaptation by hackers other than those who developed it. Such probably inadvertent propagation can be considered what Paul Virilio (2000) terms an "integral accident," a malfunction intrinsic to, and inevitable for, viral cyberweapons.[15]

Once one passes to the civilian perception of real or imagined cyberwar effects, the scope for misrecognition increases and potentially ranges from imagining wars where none exists to not noticing those that are actually raging. Zetter (2016b) reports a "misrecognized" attack on a power grid in Ukraine that occurred on December 23, 2015, when twenty-seven substations of the Prykarpattya Oblenergo, a Ukrainian power distributor that serves 538,000 customers, went dead after the company's computers were infected by a version of a high-powered web-based malware BlackEnergy 3, in what is generally regarded as an act of Russian aggression, although the attribution, as always, is inconclusive. The cyberevent attracted the attention of cybersecurity and hacking communities: the blogosphere and specialized online channels and platforms competed for the most informed interpretation of the blackout. In Ukraine, however, where the cyberattack took place, it was unnoticed, despite successfully plunging hundreds of cities and villages into darkness. With the exception of security, administration, and technical personnel of the power station, the local population took the blackout for a common power shutdown, a nationally centralized procedure aimed at saving electricity in the country's declining and war-afflicted economy.

In a reverse example, in August 2008, cyberattacks took place in the midst of a broader armed conflict between Russia and Georgia over the disputed territory of South Ossetia. Although these attacks, allegedly coordinated or encouraged by the Russian state, did not significantly affect the ongoing kinetic action, distribution of malicious software; defacement of political, governmental, and financial websites; and multiple DoS and DDoS attacks on governmental, financial, news, and media websites generated confusion and panic among the population of the country at a time when "Georgia was the most dependent on the availability of information channels" (Tikk, Kaska, and Vihul 2010, 69–79, 72). Then, on March 28, 2011, the internet in Georgia and Armenia went down for nearly the entire day after a seventy-five-year-old Georgian woman named Hayastan Shakarian, while digging for scrap copper, accidentally cut a fiber-optic cable owned by Georgian Railway Telecom that runs through the two countries (Millar 2011). It would not have been too strange if, to a traumatized wartime population, this accident had signaled another kinetic offensive (Deibert 2013, 29). How many times would such suspicions need to be shared and commented on in social networks to become someone's "knowledge"? To scale and speed up to the status of "fake news"? To serve as a useful context or leverage for a future cyberattack? To premediate an invasion?

The cybernetic autopoiesis of unplanned and undesired incidents, unavoidable and unpreventable accidents, as well as the masterminded and preplanned operations constitute the ongoing production of events and semblances constitutive of cyberwar dynamics. Everything, even what did not have place, did not happen, or was misattributed, has a positive value in the cyberwar economy. This trompe l'oeil creates blind spots in the field of vision of all observers of cyberwar.[16] It accelerates what Žižek (1999, 322) calls the "decline of symbolic efficiency" in digital capitalism. As Jodi Dean (2014, 213) explains, this develops the Lacanian idea that

> there is no longer a Master-Signifier that stabilizes meaning, that knits together the chain of signifiers and hinders their tendencies to float off into indeterminacy. While the absence of such a master might seem to produce a situation of complete openness and freedom—no authority is telling the subject what to do, what to desire, how to structure its choices—Žižek argues that in fact the result is unbearable, suffocating closure.

A "setting of electronically mediated subjectivity [that] is one of infinite doubt and ultimate reflexifisation" intensifies "the fundamental uncertainty accompanying the impossibility of totalization" in a symbolic environment where "there is always another option, link, opinion, nuance or contingency that we haven't taken into account" (Dean 2014, 212). Computational propaganda that aims to mystify invasions and occupations, or promote cynical disaffection from an adversary's political system, actively weaponizes the "decline in symbolic efficiency," but it is endemic to the whole field of cyberwar.

The extreme uncertainty and opacity of cyberwar do not, however, inhibit the interpellative effects of contending cyberwar apparatuses as they summon up cybersoldiers, patriotic hackers, vigilante militias, and security-conscious digital citizens. On the contrary, the problems of verifying or disproving multiple alarms and accusations accelerates these processes and puts them into overdrive. To put this point in psychoanalytic terms, as we noted previously, commentators on Althusser have criticized the appropriation of Lacan's theories of the subject in his account of ISAs. These critics point out that what Althusser misses in Lacan's account is that the subject is *always incomplete*; it is precisely what can never be fixed by a specific subject position or identity. However, the implication of this incompletion is not that the subject remains some untouched and primordial haven of authenticity but rather that this lack drives to ever more compulsive (because unfulfillable) attempts to attain a definitive identity. Translating this into political terms, we would say that it is the inescapably incomplete, provisional, and easily falsified nature of all accounts of cyberwar that energizes the adoption of increasingly militarized, extreme, paranoid, and unshakable subject positions vis-à-vis its alleged events.

For example, shortly after the outbreak of the rebellion that grew into the Syrian civil war, there was an abrupt but near-total shutdown of the Syrian internet. A common assumption, at least in the West, was that this was an attempt by the Assad regime to black out online dissent, as Mubarak had attempted in Egypt. But according to Edward Snowden, the event was caused by intrusion into the system conducted by the NSA—not intentionally, however, but by accident, in a botched hack of the Syrian state's communication and electronic defense system (Ackerman 2014). Whereas the first attribution cast the Assad regime in the conventional role of despotic suppressor of civil rights, rightly opposed by liberal democracies, the second reversed the significance of the blackout, making it evidence of—once again—NSA cyberaggression against foreign states, and incompetent aggression at that. But those opposed to this characterization could point out that at the time Snowden made his diagnosis, he was reliant on Russia, a supporter of the Assad regime, for political asylum. The blackout of Syria's internet connection thus also becomes an epistemological blackout about its cause, a blackout in which every initial position on the politics of Syria's civil war could be preserved and reinforced.

To provide a final example that is closer to home for many readers, as we suggested in chapter 1, there is now fairly convincing evidence that Russian intelligence agencies, whether directly or by proxy, attempted some intervention in the 2016 U.S. presidential election by way of "fake news." It is also clear that some of the news reports claiming to substantiate or expand this claim, by claiming, for example, to detect Russian hackers in Vermont's power grid or by broadly characterizing a sweepingly wide range of U.S. media outlets as accomplices of Russian cyberwar, are inaccurate and tendentious. The abyss of this double falsification—"fake news" compounding "fake news"—becomes a zero-gravity free-fire zone within which contending factions within the U.S. political system trade charges of treason, producing a civil war effect possibly beyond the wildest dreams of the toilers at the dreary offices of St. Petersburg's Internet Research Group.

SPEAKING OF DREAMS

Despite the warnings, protocols, or simply general situational awareness regarding usage of social media and mobile phones in the military zones, soldiers seem to be no different from other users, for whom sharing activities with mobile apps has become the way of living socially and communicating, disclosing one's everydayness to the network's gaze. Today, when the topic of security is trending and exploited, users can not be fully unaware of the scope of their disclosures, the associated risks and potential harm. Perhaps this is precisely what often drives the ongoing ubiquitous disclosure: exposure hurts and pleases users at the same time—the contradictory sensation that Lacan named by the French term *jouissance.*

In Lacan's terminology, the structure that hosts the alienated subject embodies "the law of the Father."[17] However, as Kittler (1997, 140) pointed out, "the world of the Symbolic [is] the world of the machine." We, too, consider that the Lacanian term can be applied to the protocological and algorithmic logic and logistics, the law and order of network operations, to which the user must submit, even if by means of pretense, in order to become *a user* in the first place. Lacan saw the subject's inability to resolve the contradictions of this dual position as nominally free, but actually unfree, as leading to the forced choice between two options: either becoming a "dupe" who enacts a misunderstanding of the system, while having some understanding of it, or a "nondupe," the one who believes in controlling the system by reducing computer to source code (think of a hacker, a corporate CEO, or the internet libertarian, fetishizing code as a solution to anything) (Chun 2008, 300).

As cyberwars intensify, digital networks become harder and more hazardous to use due to the continuous blocks, shutdowns, intrusive surveillance, new toxic malware, and so on. And yet, the internet in the mind of the majority of users remains conceived via the idea of "connection" rather than, say, "antagonism" or "collapse." The user thus enacts the imaginary relation with technology promised by commercials (the real "fake news" in consumer society). As such, the user, who is not fully unaware of the problems, yet dismisses them, is the necessary link in the cyberwar assemblage. The user is forced to act *stupidly.* This stupidity "is not always at odds with intelligence but can operate a purposeful exchange with its traits. . . . Intelligence itself depends on a withholding pattern that in some cases matches the irremediable reluctance of the stupid" (Ronell 2002, 10).

In regard to the second option of being a "nondupe," Lacan took the notion of the law and order further by tweaking it again to *les non-dupes errant,* meaning "those who do not let themselves be caught in the symbolic deception / fiction and continue to believe their eyes are the ones who err most" (Žižek, n.d.). This perfectly captures the epistemological condition in cyberwar when we have too many obvious proofs, too much information. One is tricked precisely at the moments of clarity or embracing the power granted by the network as well as at the moments of living the most "authentic" yet extremely ambiguous "carnal resonance" (Paasonen 2011) of arousal or the "real affect" of anxiety (Lacan 2016).

On one hand, the user-subject is the subject of data. To rephrase Lacan's definition of the subject (that which is represented by one signifier for another signifier[18]) in the context of information economy, the subject of data becomes that which one data point represents for another data point. Here the user is trapped in the representational data chain as negativity, as a figure of exclusion, whose place is persistently taken over by data: the subject is not present but always already represented. On the other hand, the user-subject is a "suture" that works to bridge the gaps, often by imagining connections or relations in operations of the porous "accidental megastructure" of the stack (Bratton 2016), where there are none. Here the subject appears as a figure of recursion, caught by circuits of misrecognition of patterns, as reflections or traits of imaginary identification, "rearranged" or "retranscribed" by the stochastic structure (Lacan 1997, 181) of language or that of the net.

These technological structures provide the subject with "reference points" for identification and orientation so that the subject allows herself or himself "to be fooled by these signs to have a chance of getting [one's] bearings amidst them"; the subject "must place and maintain [oneself] in the wake of a discourse and submit to its logic—in a word, [the subject] must be its dupe" (Miller 1990, xxvii). In a certain sense, of course, it is better to be a dupe of paranoia than a dupe of the technological, linguistic, or ideological system. It is precisely in recognizing one's subjective position as a dupe of the system that the subject secures a possibility of "another knowledge" upon which to act, when the system tightens its grip: "just because you're paranoid doesn't mean they aren't after you." Instead of choosing between a possibility of being paranoid or a possibility of being followed, one refuses to take these as mutually exclusive and to be divided by such choice, especially when the right option to choose *seems* apparent.

In the documentary *Lo and Behold, Reveries of the Connected World* (2016), German filmmaker Werner Herzog converses about the impact of the IoT, AI, and autonomous machines with several distinguished computer and mechanical engineers, scientists, philosophers, and entrepreneurs, including Leonard Kleinrock, Bob Kahn, Elon Musk, Danny Hillis, Sebastian Thrun, and Ted Nelson, whom he invites to share their visions of the future. And then, perhaps with a hidden intention to punctuate or disrupt his guests' technoenthusiasm, Herzog suddenly asks them an awkward question, upon which they inevitably stumble: "Prussian war theoretician Clausewitz," Herzog proclaims, "famously said, 'Sometimes war dreams of itself.' Could it be the internet starts to dream of itself?" Herzog does not explain how this reflection about war that allegedly belongs to the nineteenth-century Prussian general appears in the same sentence with "the internet," but it seems to touch what is already on everybody's mind. So, one response to Herzog's "von Clausewitz question" could be, "Yes, the internet dreams of itself—and when it does, it dreams of war." Such a dream would, however, have to be understood as akin to one on which Freud reported: a father falls asleep near the coffin of his dead child and sees his son alive, whispering, "Father, don't you see I'm burning?" Waking, the father notices the boy's dead body caught on fire from a candle (Freud 1900, 509). To Freud, the dream manifested the father's wish fulfillment, allowing him to prolong his sleep as a means of seeing his child alive. Lacan, however, argued that in dreams, where repressive mechanisms are disabled, we find ourselves in a dangerously close proximity to the unbearable real and wake up to avoid the encounter. To him, our imaginary construction of reality was the waking daydream in which we escape the real. That daydream would be our continuing reverie about the plenitude and peace of the promised digital future, while the unbearable real is war and cyberwar, burning with ever-increasing intensity.

This page intentionally left blank