DHQ: Digital Humanities Quarterly
2012
Volume 6 Number 2

Webbots and Machinic Agency

John Johnston <jjohnst_at_emory_dot_edu>, Emory University

Abstract

Malware and criminal operations performed by botnets on the Internet not only pose a new threat, but also point to our increasing reliance upon a new form of machinic agency, which I call the webbot assemblage. Whereas news media coverage of its operations considers only their human aspects, mostly in relation to crime and cyberterrorism, Daniel Suarez's recent novel *Daemon* provides a suggestive glimpse into how, in a webbot assemblage, new forms of human and machinic agency are complexly intricated. The significance of this assemblage becomes further evident when it is considered in relation to how the Internet is increasingly perceived: no longer as a neutral medium but as an ecosystem defined by netwar, software arms races, and the possible evolution of “low” forms of artificial life.

Introduction

In recent years, sophisticated new forms of cybercrime and cyber warfare have displaced spam, pornography, and vandalistic viruses as the most visible threats from the Internet's “dark” underside.[1] As early as 2003 and increasingly from 2004 to the present, the primary use of computer viruses and worms has been as malware, which is used to break into and capture networked machines and data systems for specifically criminal, money-making purposes, or for politically subversive or destructive ends. Sometimes these subversive actions have taken a positive political turn, as when they participate in the ongoing efforts to maintain free and open access to the exchange of information, or to expose the secret and illegal actions of surveillance, whether by state or private data-mining agencies. The hacktivists' attacks against companies like PayPal which tried to weaken or end financial support for WikiLeaks in the wake of its release of diplomatic cables was one spectacular instance. Stuxnet, the worm that penetrated and corrupted the computer system controlling the centrifuges of the Iranian nuclear enrichment program, provides a comparably dramatic example of cyber warfare.[2] Shortly after reports of Stuxnet appeared in the news media, the former anti-terrorist security advisor for Presidents George W. Bush and Bill Clinton, Richard A. Clarke, published *Cyber War* (2010), a book detailing the increasing vulnerability of the American government, military, and large corporations to cyber attacks launched by State hackers working for foreign governments. But in fact, news reports of cyber war have generally been less frequent, and mainly of interest to Internet security experts. The vast majority of related news media stories for the past six or seven years concern the exploits of cybercriminals, and have focused on Distributed Denial of Service attacks, instances of extortion, identity theft, and the astronomical sums of money invested in Internet security and extracted by mafia-supported hackers. These reports have been so visible, in fact, that President Obama felt compelled to give a public speech about cyber threats and the costs of cybercrime early in his presidency.[3]

1

While certainly justified — indeed, to ignore Internet security and the dangers of malware would be foolish — this media attention is concerned almost exclusively with “the human face” of a vast technological assemblage whose machinic operations mostly remain obscure. Specifically, our greatly increased dependency on the Internet necessarily also means our increased dependency upon a variety of “bots” (software robots) and intelligent agent software more generally. Much of what happens on the Internet is enabled or carried out by web bots, spiders, screen scrapers, and many quasi-autonomous software systems. Although essential to the functioning of our current information society, the new forms of machinic agency that bots instantiate have received very little critical attention outside the circles of

2

Internet security and data mining professionals. Here, I will examine what I call the webbot assemblage from multiple, partially overlapping perspectives – first, new malware and Internet security, second, a contemporary cyber-thriller in which a webbot assemblage figures centrally, and third, the dynamically changing nature of the Internet itself. My aim is to sketch a new understanding of the evolving and complex imbrication of human and machinic agency that the Internet is bringing about. Indeed, the developing technology of the webbot assemblage is inseparable from many of the dynamical changes we have witnessed in the Internet itself over the past decade or so, as it has acquired the traits of an ecosystem defined by netwar, software arms races, and the possible evolution of "low," barely intelligent forms of artificial life.

Bots on the Net

3 Unlike the computer voices on the telephone with which we frequently interact, most bot activity remains invisible. In eerie silence, countless numbers of bots tirelessly search for, record, retrieve, sift through, and act upon the ever-enlarging masses of data without which our contemporary high-tech world could not function. While most of this activity occurs on the Internet, it is instigated by and purportedly serves the interests of people at the "front-end," in offices and at desktops everywhere. Much of financial management, for example, is automated by bots, which more and more often determine whether or not we get a loan or mortgage. Bots scan x-rays and MRIs, function as players in online games and as purchasing agents for brokerage houses. They operate and monitor surveillance cameras all over the globe, as unblinking eyes that watch and record many of our activities — our movements, spending habits, commercial transactions, and health records — which other bots in turn analyze for patterns which are then sold on the market. The massive increase in cell phone and e-mail surveillance since 9/11 would not be possible without bots. In fact, the Internet itself, which we commonly think of as a network of people using machines, is increasingly used for machine-to-machine exchange, specifically Electronic Data Interchange (EDI). In sum, Internet bots now automate a widening range and number of activities that until recently only humans could perform.

4 Initially, bots were a basic tool for network maintenance and data management. But with the Internet's accelerated use and expansion in the late 1990s, bots were developed that could search the Web, download pages or selected bodies of information following refined search criteria, and then bundle it neatly in a file for the human user.[4] This type of bot, usually called a web crawler, systematically visits web pages, retrieves content, extracts URLs to other relevant links, and then in turn visits those links. In addition to data mining, web crawlers are often used to find and repair broken links. But they can also be used to retrieve user information, including usernames and passwords, as well as security information about the user's machine or system. Consequently, bots have also become a primary means for malicious and criminal exploits, the most threatening of which is their collective formation in criminal "botnets."

5 In its simplest form, a botnet is an army of compromised computers that takes orders from a "botherder." In *Botnets: The Killer Web App*, Craig Schiller et al explain further: "The software that creates and manages a botnet makes this threat much more than the previous generation of malicious code. It is not just a virus; it is a virus of viruses. The botnet is modular — one module exploits the vulnerabilities it finds to gain control over its target. It then downloads another module that protects the new bot by stopping antivirus software and firewalls; the third module may begin scanning for other vulnerable systems" [Schiller et al 2007, 3]. To start this process, a hacker first tricks the user into installing a root kit that gives him (they are still mostly males) complete control over the user's machine. Several vectors are used to install such malware: getting the user to open a contaminated email or to download software from a compromised website are the most frequent. To penetrate databases storing credit card and personal information of large numbers of people, hackers often deploy software tools to probe for open or unprotected ports through which the malware is downloaded directly.[5] With malware installed, the hacker or botherder — completely unknown to the user — can use the compromised machine or "zombie" to send waves of spam or pornography, or else enslave it in huge botnets that are mobilized in Distributed Denial of Service (DDoS) attacks, which overload and crash the target website, rendering it inaccessible. Initially such attacks were directed against online gambling sites and large corporate web sites, but more recently all sorts of organizations and even governments have been targeted. In *Fatal System Error* [Menn 2010], Joseph Menn provides many detailed examples of how DDoS attacks have been used for criminal extortion by mafia-like organizations in Eastern Europe and Russia. As Menn shows, these highly skilled and well-paid criminal hackers

rely on networks of semi-secret websites that offer malware and services like pay-for-use botnets. Such “darknets” constitute an extensive network of underground sites used to develop and market the essential tools of the trade.

6 One significant side effect of these DDoS attacks has been to make more visible both the power of bots and our greatly increased dependency upon them. The problem of countering the threats they pose will be considered later; here let it suffice to note that with the constant development of Internet security measures we are witnessing an escalation of the “malware wars,” which are usually represented as an evolving software arms race between “the good guys and the bad guys,” with the future of the Internet at stake. These developments — and foremost the greatly increased sophistication of the tools that now make up criminal webbot assemblages — indicate an important historical shift. This is evident in the large numbers of criminal hackers, their complex organization, and often the concerted nature of their actions, which sharply contrast with the practices of the preceding epoch, when only small numbers of relatively isolated hackers wrote and launched computer viruses for vandalistic, anti-social motives or simply to experiment with software “in the wild.”

7 This historical shift to large criminal organizations and thus to a well-financed criminal hacker class whose motivation is purely monetary or economic is not the whole picture, however. Many recent events suggest that the line between the mafia hacker and the State-supported hacker is becoming blurred. In his book, Inside *Cyber Warfare: Mapping the Cyber Underworld*, Jeffrey Carr cites a number of relevant incidents. When Russia attacked Chechnya in 2002, for example, it used some of the same criminal organizations just mentioned to bring down Chechnyan opposition websites. In 2001, when Chinese and American military aircraft collided over the China Sea, thousands of Chinese hackers spontaneously launched a “counter cyber-offensive” against US aggression. As a result, as Carr puts it, “non-State hackers [have become] a protected asset” [Carr 2010, 29]. Yet, since the evidence suggests that many nation-states besides China and Russia not only tolerate but actively support and even provide university or technical training for hacker groups, a clear and constant distinction between state and non-state hacker can no longer be maintained. Perhaps a more appropriate framework could be extrapolated from Gilles Deleuze and Félix Guattari's concept of “nomad war machines,” which, they theorize, have always existed apart from but can also be appropriated by a State apparatus.[6] In many of the instances cited by Carr and Clarke, malware and rootkits functioning in webbot assemblages have clearly been weaponized for cyber warfare by nation states.

8 The Stuxnet worm provides a highly instructive example. Its apparent purpose was simple: to slow down Iran's production of high-grade uranium by destroying the functionality of its centrifuge machines. However, Stuxnet represents a striking leap forward in complexity and functional design. Based on a rootkit and multi-functional set of software modules much like the criminal botnet assemblage described earlier, it adds a large array of components to increase its chances of success — for example, it exploits several “zero-day” Windows vulnerabilities (i.e. vulnerabilities still largely unknown to software developers and for which no security fix has yet been issued by vendors), it increases the number of possible infection paths, includes new antivirus evasion techniques and two forged digital signatures, and it can be easily updated and possesses a command and control interface.[7] Basically, Stuxnet targets with laser-like precision a Siemens industrial control system, invisibly rewriting the code and altering the variables for the centrifuge engine speeds, which this system regulates. This very capacity to target a single mechanized unit within a complex industrial control system at a precise physical location — rather than a specific website — makes Stuxnet a fearful development in the hacker's armory of tools and software weapons. The workings of Stuxnet forcefully demonstrate that webbot assemblages can be used not only to gain access to valuable and protected information but also to penetrate into and manipulate physical machines and industrial control systems in acts of netwar.

An Internet Daemon

9 The kind of multi-functionality now evident in webbot software is dramatically illustrated in Daniel Suarez's popular cyber-thriller, *Daemon* (2008).[8] Since the novel clearly delineates some of the central features of the webbot assemblage and its machinic operations, it is worth examining in some detail. Conspicuously concerned with the blurring of the human-machinic interface and the becoming autonomous of a highly distributed system, it suggestively presents a diagram of how human agency — precisely by means of the webbot assemblage — is disassembled into part-functions and re-distributed into what amounts to a new, collectively functioning posthuman form. As Suarez later

revealed, the novel's central idea originated in his work developing software systems. After developing an application for changing the weather in computer games, he made it available to download on the Internet with an automatic pay system. After several years, he noticed that it had deposited a tidy little sum into his bank account. He then began to imagine other things that you could do even if you were dead. The basic idea for the novel soon followed. Its overarching plot centers on a talented online game designer, Matthew Sobol, who contrives to set in motion after his death armies of bots directed by a sophisticated AI game engine. Guided by “the Daemon,” as this new form of machinic agency comes to be called, the bots carry out increasingly complicated scenarios. First, they recruit several human agents, including a journalist who helps to disguise the Daemon's murderous and destructive actions by shifting the blame onto an investigating police officer whose supposed theft of Sobol's money is publically “exposed.” Almost invisibly, armies of bots then remorselessly begin to dismantle our current society and reconstruct it as a fully distributed, automated system.

10 An unlikely event triggers the novel's initial action: two of the leading programmers at Cyberstorm Entertainment, a highly successful producer of Internet games, die of what first appear to be high-tech accidents. One has his throat slit by a wire that rises up across the path where he normally rides his motorcycle; the other is electrocuted when he tries to enter the company’s data center and possibly shut down the servers. However, the ensuing police investigation reveals that these deaths are very sophisticated, automated executions. Proceeding slowly and methodically in the face of the skepticism and technical ignorance of the “higher ups” in the police department and FBI, the local homicide investigator and a computer consultant who is initially a suspect piece together evidence of an unprecedented new type of plot in progress. It turns out that Matthew Sobol, the wealthy and inventive game designer who had founded and controlled Cyberstorm, had recently died of brain cancer. For reasons never fully disclosed, Sobol had programmed bots to scour Internet news sources for the announcement of his own death, and then, in response to this announcement, to set in motion a vast complex of orchestrated events, including the destruction of the FBI agents who attempt to search his California mansion. The novel renders this attempted search-turned-siege as a vivid action sequence. The house is defended by a bot-controlled, weaponized Hummer programmed to hone in on the heat signatures of the FBI agents; inside, it is booby-trapped with high tech weapons like subsonic broadcasts that leave the attacking SWAT team writhing in nausea. Later in the novel a whole fleet of autonomous vehicles will be built according to online specifications and will constitute a mechanized army ready for attack.

11 Much of the novel's action is made possible by Sobol's modification and deployment of the software he had developed for his hugely popular Massive Multiplayer Online Role Playing Games, “Over the Rhine” and “The Gate.” To implement his manipulative game scenarios, Sobol had invented a powerful AI game engine (called “Ego”), which he has adapted so that it can coordinate the activities of a huge "darknet" of bots and other robotic agents, and which eventually includes human agents. To enlist the services of the latter, particularly his devoted gamers, Sobol has also modified the game map and special graphical user interface developed for the online games. In another vivid action sequence, a criminal hacker named Brian Gragg, who is also a highly skilled player of “Over the Rhine,” engages in combat with German troops led by the fearful Nazi Lieutenant Boerner, a game character who acquires a quasi-autonomous “life” of his own as a “recruiting avatar.” After one of their combat encounters, Boerner leaves Gragg an encrypted clue that will unlock this special interface, after which Gragg is led to take intelligence and skill tests and then recruited by the now dead Sobol, who appears to Gragg in a video made before his death.

12 Gragg is only one of many among the criminals, the disaffiliated, and the out of work who are similarly induced to join Sobol’s secret network. Membership gives them access to this special graphical interface from “Over the Rhine,” expanded to include an integrated Global Positioning System to map and coordinate both human and bot resources. As the hacker Jon Ross explains to the FBI investigators, “In essence Sobol is using the GPS system to convert the earth into one big game map. We're all in his game now” [Suarez 2008, 358]. Ross and the FBI then discover that the new interface projects a virtual overlay onto the agent's environmental space (this requires a wearable computer and special contact lenses) in which “call-outs” identify human agents to one another and the resources that are locally available. Beginning with the actions of bots and progressing to multiple, hybrid forms of agency operating at several levels, Sobol's online games become an autonomous network whose agents begin to penetrate into and transform social, economic, and political reality.

In effect, Sobol's online game world functions as a transformational matrix for bringing about a fully distributed and automated society, initially engineered by webbots and other robotic agents that collectively constitute a remorseless machine — the “Daemon” of the title. In computer technology, a “daemon” refers to a small computer program or routine that runs invisibly in the background, usually performing house-keeping tasks such as logging various activities and responding to low-level internal events. Analogously, the reader of the novel doesn't directly perceive the actions of the webbots, only humans carrying out their instructions — for example, at a small firm where engineers are converting newly purchased SUVs into autonomous vehicles according to specifications received online from an outsourcing company. Over the course of the novel this Internet daemon extends its reach into an increasing number of production and distribution networks, and thus into the economy at large, slowly and systematically dismantling and rebuilding the world according to a ruthless logic of efficiency and highly distributed, low-level intelligence. By the novel's conclusion, the Daemon has infiltrated and taken over the databases of many large corporate and financial institutions, and successfully frustrated the government's efforts to defeat it. 13

Bots as Narrow AI and Artificial Life

Whereas the idea for *Daemon* stems from the author's technical interest in the efficacy of bots, its realization reflects a worry about the possible consequences of their increasing capacity and our developing dependence upon them. In interviews Suarez has insisted that his novel is not a sci-fi scenario, since the necessary technology already exists. Yet, clearly no Luddite, Suarez is hardly interested in denying the conveniences bots provide, or the labor and tedium they enable us to avoid. His concern, rather, is with the layering and the extent of automation that bots are making possible, and as a consequence the tendency to reduce the number of people making the important decisions that both directly and indirectly affect human lives. In other words, he is worried by the possibility that bots are becoming a form of autonomous agency inimical to the public good. 14

In a web-cast lecture entitled “Bot-Mediated Reality,” [9] Suarez focuses on our current society's collective pursuit of hyper-efficiency, arguing that bots are the perfect tool for its achievement. Cheap to make and operate, bots are relentlessly efficient, for unlike the humans they replace, they have very few needs. As evidence of their ascendance, Suarez points to the exponential increase over the past few years in the number of bots, the amount of malware, the size of hard-drive space on our computers, and thus the growing size of an ecological niche for software agents. While bots could certainly become a vector for human despotism, the greater danger, he thinks, would be the collective human loss of control over society: since bots could enable society to function as a vast inhuman machine on auto-pilot, its operations would no longer be susceptible to human steering. Human beings, as large-brained animals with complex motivations not reducible to efficiency, would then have created an environment in which they no longer enjoy an adaptive advantage, in a sudden reversal of human history. Thus Suarez summarily suggests that this desire for hyper-efficiency has led to and may be locking us into a Darwinian struggle with low or narrow AI, specifically with the kind of low-level intelligent software instantiated in bots.[10] 15

To be sure, Suarez is not the first or only one to wonder if bots might constitute a new form of machinic life.[11] One of the first books to consider bots, Andrew Leonard's *Bots: The Origin of a New Species* (1998), explicitly raises this possibility.[12] Leonard, however, does not pursue what may be the most intriguing corollary to this possibility: that bots are a new form of digital parasite, like the *sacculina* parasite that slowly converts the sand crab into its own zombie reproductive machine. As a silicon species whose number has grown over two thousand per cent in the past few years and now enjoys a rapidly expanding ecological niche, bots could become — or may be becoming — the agency of a double transformation, providing both a mechanism that could enable our society to operate on auto-pilot, as a hyper-efficient machine no longer under human control, and, as a form of “low-life” intelligence, the medium and environment in which network agency could evolve to greater complexity. This double transformation, moreover, points to a specifically “machinic” aspect of the webbot assemblage. In effect, it evolves through the doubling back on itself or retroaction of a cybernetic loop: humans build and deploy bots in an extension of human agency, but — from a reversed perspective — the bots also reproduce and evolve by means of the human desire to build more and better bots. When a certain threshold is achieved — that of an autonomous technology — this language is no longer metaphorical, but simply indicates how an assemblage of human and nonhuman agencies has become self-sustaining and self- 16

perpetuating.[13]

17 *Daemon* is explicitly concerned with the first aspect of this double transformation, but not with the further evolution of bot technology. It can thus be read as a cautionary tale, comparable to Michael Crichton's techno-thrillers like *Jurassic Park* and *Prey*, where hubristic humans deploy a new technology that quickly escapes their control. At the same time, and this is the source of its deeper interest, *Daemon* offers a fundamentally different kind of narrative, one driven by a peculiar transformation and displacement of human agency: having (posthumously) set the webbot assemblage in motion with the announcement of his own death, Sobol survives or "lives on" as a form of artificial or machinic intelligence through the operations that the webbots collectively perform. As a consequence, Sobol's relationship to his "daemon spirit" appears as complexly ambiguous. At once a posthumous and "posthuman" figure, the Daemon is not the cause but the result of the bots' collective and emergent actions. At the level of Sobol's programmed bots, there is no "human face" or purpose — only an operational logic extending along vectors of a vast communicational network, in effect defining a virtual plane of immanence actualized in a multitude of highly distributed parallel actions. Working *only* at this level, this autonomous and remorseless form of agency is intensely corrosive of large hierarchical organizations like contemporary corporations and the US government, which require repeated attributions of meaning and purpose at every level precisely because they operate through (while also transcending) individual human connections. Having no inherent purpose beyond their own local functionality, the bots collectively produce an emergent, global effect — the dismantling of current corporate society — simply by working in concert at the lowest level of machinic efficiency.

18 Thus, while "the Daemon" is denominated as such by Sobol and assigned this role as immanent and material cause by Sebeck and the other characters, this totalizing effect should be understood as a metaphor, as the novel's symbolic staging of the way humans "make sense" of a complex transformation, in this instance of how Sobol's bodily human intelligence has been extended into and replaced by the concerted actions of thousands of little intelligences at work, as if they were swarms of robotic homunculi. In other words, the Daemon provides a convenient fiction by which a unified and transcendent agency can be attributed to the "low-life" actions of a highly distributed intelligence that is re-making all complex, hierarchical organizations and structures in its own "flat" image. This diffraction or gearing down of human agency into lower machinic levels is represented as initially violent and destructive, in keeping both with the violence of Sobol's first-person shooter games and the literary genre of techno-thriller fiction. However, it is ultimately not all bad news for humans, who are quite capable of living productively in flat, web-like networks instead of large scale, corporate hierarchies. Indeed, such flat networks may well be the necessary bedrock of a more sustainable human future, as *Daemon*'s sequel, *Freedom* (2010), suggests.[14]

Netwar and New Agency

19 We can now consider from a wider perspective what Suarez has extrapolated from our contemporary hi-tech world that requires this embedding of the webbot assemblage and its particular form of agency in his fictional narrative. We shall see first that it is *not* at the level of agent software and the swarms of bots running on the Internet that the novel's primary fictionalization occurs. Rather, it is more globally, at their targeting of the structure and mode of operation of corporate capitalism and its servant (or handmaiden) the nation-state. In *Daemon* all the robotic attacks are directed either at corporations that "reside" in the US or at the US government — indeed, sometimes these two entities are blurred. In 1886, the US Supreme Court declared that corporations were "persons" entitled under the Fourteenth Amendment to the same protections as living citizens. But as Peter Barns in *Capitalism 3.0* points out, following many others before him: "... the modern corporation isn't a real person. Instead, it's an automaton designed to maximize profit for stockholders. It externalizes as many costs as it possibly can, not because it wants to, but because it has to. It never sleeps or slows down. And it never reaches a level of profitability at which it decides, 'This is enough. Let's stop here'" [Barns 2006, 23]. Barns' specific terms should make it clear that Sobol's Daemon is meant to mirror the automaton that is current corporate capitalism; or rather, it is the latter's inverse or "demon" image, since profit is not its motive. The Daemon's purpose, rather, is only to perpetuate itself as a fully distributed agency with no central authority and thus as an inversion of the corporate structure.[15] It can achieve this, however, only by converting the webbot assemblage into a war machine. In other words, it can enact and fully become a completely distributed agency only through all-out netwar against the highly centralized and hierarchical agencies of the corporate state.

In the 1990s, two researchers for the Rand Corporation, John Arquilla and David Ronfeldt, defined netwar as “an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age” [Arquilla and Ronfeldt 2001, 6]. Arquilla and Ronfeldt emphasize two particularly relevant aspects of netwar. First, “Hierarchies have a difficult time fighting networks,” and thus “It takes networks to fight networks” [Arquilla and Ronfeldt 2001, 15]. Those who practice netwar — the authors mention “criminals, terrorists, or peaceful social activists” as specific “adversaries” — therefore operate as completely dispersed nodes or “multi-channel” cells, in either case as part of de-centralized or highly distributed networks without central command and control structures; instead, they are “headless” or “hydra-headed” and allow for local initiative and autonomy. Second, a frequently deployed tactic for attack in netwar is the use of swarms or a massively large number of agents that can simply overwhelm the enemy. Whereas the terrorist organization Al-Quaeda serves as an obvious example of the first feature, the massive swarms of bots deployed in actual Distributed Denial of Service attacks clearly exemplifies the second. 20

Both of these features are fundamental to the netwar carried out by Suarez's *Daemon*. It should be noted, however, that the Daemon itself doesn't fit precisely into any of Arquilla and Ronfeldt's categories of adversary, but partakes ambiguously of all three. The authors' comments on what they call the “darkside” and “the ambivalent dynamics of netwar” are revealing in this respect. They see the type of conflict they call netwar in relation to a specific, historically repeating pattern: “a subtle, dialectical interplay between the bright and dark sides in the rise of a new form of organization” [Arquilla and Ronfeldt 2001, 313]. Summarily, whenever new forms of organization emerge, so do “bad guys” on its cutting edge, who are often eager and very quick “to take advantage of new ways to maneuver, exploit and dominate” [Arquilla and Ronfeldt 2001, 313]. The “good guys,” in contrast, “may be so deeply embedded in and constrained by a society's established forms of organization that many have difficulty becoming the early innovators and adopters of a new form” [Arquilla and Ronfeldt 2001, 313]. Involving both a new form of organization and new technologies, "the network form" brings new risks and dangers; specifically, the authors note, threats to freedom and privacy. Furthermore, as an “ambivalent mode of conflict” with a dual nature, netwar can be expected to “cascade across the spectrum of conflict and crime” [Arquilla and Ronfeldt 2001, 314] as the information revolution spreads globally and its technology grows more sophisticated. However, the radical increase in connectivity — which actually blurs the distinctions between the local, the transnational, and the global — also means that “insiders” and “outsiders” are no longer so easily separated or even identified. And far from being a transitional phenomenon, it will likely be a “permanent aspect of the new era” [Arquilla and Ronfeldt 2001, 315]. 21

The problem evident here, however, is that Arquilla and Ronfeldt assume that specific types of human subject (“good guys” and “bad guys”) already exist and are simply called forth by the emergence of new forms of organization, that the “bad” subjects then appropriate these new forms for their own antagonistic ends. As a consequence, the authors remain bound by a static and essentialist conception of human agency. I suggest, to the contrary, that the advent of a new form of organization and a new technology — and it is not evident that either of these ever occurs separately — alters the very nature of human agency and thus our understanding of the human subject. Specifically, as new technology both elicits and creates new possibilities of agency, a corresponding zone of subjective indetermination is also created. In the new age of digital connectivity — point and click, cut and paste, rapid information searches and scanning — in which writing and using code, adapting to completely mobile communications and collectively participating in online gaming and “social media” are all new forms of action, the technology transforms what it connects. Specifically, the putatively human subject is first and foremost (re)defined operationally as a dense node of complex and adaptive functionalities in multiple networks, and thus a site of uncertain affects, stoppages, and transductions. These operate as neither simple mechanical transmissions of force nor as exchanges of meaning, but as both at once, as entanglements and comminglings in which agency is not only multi-mediated and multi-modal but viral and memetic. In a technological network society the human is never fully separated from the nonhuman and the machinic — there are only “degrees of separation.” 22

In effect, human agency diffracts into multiple, interacting sub-agencies — many of which are nonhuman — only to be (but not always) re-assembled in entirely new configurations and aggregates. In the primary example developed here, a particular set of human and machinic agencies working together defines the webbot assemblage. What I called at the 23

outset the “human face” of this assemblage can now be understood (like Sobol's *Daemon*) as a passing but inevitable attempt to maintain the appearance of a human unity and continuity, by projecting the full dimensionality of human action onto a scene where it has actually been diffracted into multiple mechanisms and emergent effects. With this in mind we can return to our point of departure, in order to consider the threat of cybercrime and to understand why it is not in any simple sense just another type of netwar.

Malware Wars

24 In the past few years professional Internet security analysts have become increasingly alarmed by the sophistication and mounting costs of criminal activities on the Internet. A 2007 issue of the journal *Computer Economics* reported that costs were averaging around 15 billion dollars a year, but added that these are only reported costs, with many companies and institutions (especially banks) not releasing information because it could hurt their reputation for being well protected.[16] In a recent series of workshops on “the Malware Wars” at the Santa Fe institute, representatives from the FBI, academic computer scientists, and security specialists from companies like Google and Symantec quickly arrived at full agreement on several fact-based issues: first, that the accelerated development of malware was driven by huge profits, and financed mostly by criminals residing outside the US, particularly in Russia, Eastern Europe, and China, where there are few if any laws or regulations; and second, that these criminals are highly organized and constantly innovating, sharing, or selling new malware to one another and often working together, especially on large Distributed Denial of Service (DDoS) attacks.[17] Moreover, many of the workshop attendees were openly pessimistic – not only because “the good guys” are way behind, always playing defense or catch-up against ingenious new software and tricks, but because of the very nature of the problem. As one put it: “One software bug or weakness equals millions of compromised hosts.” Another was equally blunt: “The rate of evolution is so much higher. Malware has such a high evolvability, it may evolve to the point that the Internet is no longer useable.” In sum, not only was there full agreement that evolvability and system robustness are the key issues, but few of the attendees had any problem accepting the assumption that “[software] programs behave enough like organisms that some lessons from nature might be applicable to the Internet and malware.”

25 The upshot of this perspective is that we are not only witnessing but, to varying degrees, participating in an escalating evolutionary arms race between attacking and defending software systems. The hope, explicitly stated at the Santa Fe workshop, is that the “good guys” will prevail by keeping the operational costs of defending systems within reasonable limits, and thus at least stabilize the situation until a more robust and less vulnerable Internet can be evolved. But of course, arms races are inherently unstable and thus unpredictable.

26 Two recent developments provide direct evidence. First, as reported in ComputerWorld Security, a new feature called “Kill Zeus” has been added to the software toolkit “Spy Eye” currently used by Russian botnets.[18] (Zeus is a more widely deployed, rival toolkit also used by Russian botnets.) While both Spynet and Zeus are designed to set up botnets that specialize in stealing online banking credentials, the new “Kill Zeus” feature allows Spy Eye to displace its rival by deleting it from zombie machines and then assuming the latter's functions. For some time now botnets have been very sophisticated, deploying modular, multi-functional, and increasingly adaptive software. Once installed on a machine, this software can download other components, search for other machines to capture, or be directed to attack specific targets in massive DDoS attacks. The new “Kill Zeus” feature (which no doubt has been duplicated in other rival toolkits) brings about a new level of complexity, by allowing these systems (or certain of their component modules) to turn each other on and off. In keeping with the analogy with biological systems, this can be likened to the actions of genetic regulatory networks, in which genes switch each other on and off, producing complex adaptive systems that evolve or don't, depending on whether new features (i.e. sub-agencies) enhance the capacities of the larger systems within which they operate. Whereas software operating on the Internet has often been compared to neural circuits in the brain performing specific computational tasks, this new “genetic” component in the webbot assemblage clearly produces additional variations and thereby increases its evolutionary potential.

27 As already noted, these systems are constantly subjected to new evolutionary pressures. We see further evidence in another development reported in *ars technica*.[19] The article points out that botnets are increasingly being used for

“ideological” and politically motivated attacks, citing recent DDoS attacks against Australian government websites by anti-Scientology groups incited by the government's plan to block access to pornography on the Internet. But it also reveals that new tactics are being deployed in botnets to avoid detection and thus circumvent defense measures. Heretofore most successful DDoS attacks owe their success to sheer numbers, often involving fifty or sixty thousand zombie machines. Of course, the sheer size of these botnets makes their attacks highly visible. The article notes a new tendency to reduce this visibility — to attack in many irregularly-timed pulses (“throttling”, rather than employing a few massive waves), at a much wider bandwidth of IP addresses, and, perhaps more significantly, to employ camouflage by encrypting the operational scripts in innocent-looking data. These new tactics, thus far, have proven to be extremely difficult to defend against. We can therefore expect a new tendency to assemble smaller, smarter, and less visible botnets, which will in turn demand new and perhaps different kinds of defense and counterstrike measures. The more recent revelations about Stuxnet, and in particular its precise targeting capacity and officially unassignable origins, only aggravate the situation, enabling the murky world of cyber warfare to transition rapidly into a potentially global and highly destructive battlefield.

Conclusion

While the escalation of the “malware wars” has been represented as a technological arms race between “the good guys and the bad guys,” with the future of the Internet at stake, the actual discourse necessary for understanding the complex dynamic of interactions at work has been that of biological ecosystems and the survival and evolution of complex adaptive systems. This conceptual disconnect is surely evidence that the concepts of netwar, cybercrime, and even cyber warfare remain too dependent upon conventional and unquestioned notions of human agency, in which the capacity for intentionality, self-awareness, and control remain uppermost. But meanwhile, on another scene — should we call it a form of “technological unconscious”? — new and different forms of agency are at work. Unfortunately, conventional notions of human agency neither provide a reason for considering the complex dynamics of the webbot assemblage or even the Internet itself as a conglomerate assemblage, nor do they instigate any interest in recognizing the rapidly developing forms of artificial life and intelligence we are busy surrounding ourselves with and indeed building ourselves into. Unless we analyze the software assemblages in which these processes are instantiated, we shall fail to perceive and understand the diffraction of human agency into the mundane, barely intelligent bots and botnets that operate on and are changing the very nature of the Internet.

Notes

[1] On viruses, see [Parikka and Sampson 2009]. My essay in the same volume [Johnston 2009] considers computer viruses mainly as experimental and vandalistic. The present essay is more directly concerned with the historical shift to the widespread use of *malware* in hacking. A general term for “malicious software,” malware includes viruses, worms, trojan horses, spyware, rootkits and other software designed to “exploit” vulnerable computer networks.

[2] The Stuxnet worm was first detected in the summer of 2010 by Internet security experts around the world, but no one knew precisely what its target and payload were. As it replicated and spread, it seemed to be searching through computer systems for a pre-defined target, which it apparently located in the Fall. Thus far there has been no conclusive determination of its origin, though the consensus opinion of security experts is that it most likely originated in a joint American-Israeli intelligence operation. I discuss some of Stuxnet's technical features further below. For more background information, see “Stuxnet: Dissecting the Worm” [Adhikan 2010]. “Stuxnet: Fact vs. Theory” [Mills 2010] summarizes many of the early news reports, and Michael Joseph Gross' article for Vanity Fair provides a useful narrative account [Gross 2011].

[3] The speech (see [Obama 2009]) was delivered on May 30, 2009.

[4] See [Cheong 1996] for a detailed discussion of Internet bots in the early 1990s.

[5] For further details on how these software tools work, see [Hogland and Butler 2006] and [Davis et al 2009]. Together with Schiller et al 2007, these sources provide a clear technical description of the botnet assemblage.

[6] See [Deleuze and Guattari 1987, 321–423] for their theory of the nomad war machine and the State apparatus. The authors insist upon the exteriority and irreducibility of the war machine vis-a-vis the State apparatus, which can “capture” but never fully “internalize” the war machine. Significantly, among the latter's many attributes and associations, secrets and betrayal figure largely. However, in the contemporary context the

primarily technical aspect of war machines and the importance of code assume a significance not discussed by Deleuze and Guattari.

[7] For details, see the extensive (70-page) analysis of Stuxnet's component software and mode of attack and operation made available by Symantec Security Response [Falliere, Murchu, and Chien 2011].

[8] See [Suarez 2008], as well as the sequel, [Suarez 2010].

[9] See [Suarez 2008b] for the complete lecture.

[10] Interestingly, the low-level AI of the Google search engine has recently begun to generate a comparable anxiety, though not (to my knowledge) on Suarez's part. For a specific example, see [Carr 2010b, 171–176]. From the outset, Google founders Larry Page and Sergey Brin were always forthright not only about the AI origins of their original search engine but also about their vision of the perfect search engine as constituting full AI. “Artificial Intelligence would be the ultimate version of Google” Page said in 2000; and in 2003: “The ultimate search engine is something as smart as people —or smarter” [Carr 2010b, 171]. What seems to have blunted or displaced public worry about this explicit development of AI is the Google search engine's widespread (and even necessary) usefulness, as well as Google's heretofore generally beneficent image.

[11] For a discussion of the concept of machinic life, see [Johnston 2008].

[12] While the population of bots — chatbots, computer game bots, and of course the bots I consider here — has vastly increased since the publication of Leonard's book, unfortunately there has been no update or comprehensive book devoted to this vital topic.

[13] In *Erewhon* (1872), Samuel Butler provides the first description of how machines reproduce by means of human agency. Langdon Winner's book *Autonomous Technology* (1977) extends Jacques Ellul's argument (in *The Technological Society*) that “technique has become autonomous” and operates beyond the control of human agency. These different strands come together in George B. Dyson's Darwin Among the Machines: The Evolution of Global Intelligence, where he writes: “Everything that human beings are doing to make it easier to operate computer networks is at the same time, but for different reasons, making it easier for computer networks to operate human beings” [Dyson 1997, 10]. The overarching determinist argument evident here — that human beings make technology that eventually produces human beings who desire only and exactly more of this same technology — depends however on a single, tightly closed cybernetic loop. Thus it is far too simple an account of the relationship between humans and the technologies they construct. In actuality, this relationship is constituted from a multiplicity of such interactive loops (or coupled dynamical systems), with any number of contingencies and indeterminacies. To speak of causal determination in the human brain alone, for example, is made exceedingly difficult by the fact that many (possibly most) neural areas are linked by both feedback and feedforward neural pathways. No doubt there are many circuits of “continuous reciprocal causation” (Andy Clark's felicitous phrase) between humans and their technologies, but many of the loops are open, inevitably expand the possibility space, and hence spiral out into indeterminate futures.

[14] For example, in *Freedom* a number of scenes are devoted to the efforts on the part of several small, networked human communities to provide an alternative to corporate monoculture and specifically to agribusiness in the Midwest.

[15] At the very end of the novel, Sobol explains to Sebeck (in a video Sobol made before his own death) that the Daemon “is a remorseless system for building a distributed civilization. A civilization that perpetually regenerates. One with no central authority” [Suarez 2008, 426].

[16] In [Obama 2009] President Obama estimates the global costs to have risen to one trillion dollars a year.

[17] See [Jackson 2008, 23–26]. The quotations that follow are taken from this article.

[18] See [McMillan 2010], accessed 10 February 2010.

[19] See [Johnston 2010], accessed 14 February 2010.

Works Cited

Adhikan 2010 Adhikan, Richard. *Stuxnet: Dissecting the Worm*. 2010. http://www.technewsworld.com/rsstory/70622.html?wlc=1306526157.

Arquilla and Ronfeldt 2001 Arquilla, John, and David Ronfeldt. *Networks and Netwars*. Santa Monica: RAND, 2001.

Barns 2006 Barns, Peter. *Capitalism 3.0*. San Francisco: BK Publishers, 2006.

Carr 2010 Carr, Jeffrey. *Inside Cyber Warfare*. Sepastopol: O'Reilly Media Inc., 2010.

Carr 2010b Carr, Nicholas. *The Shallows: What the Internet is Doing to our Brains*. New York: Norton, 2010.

Cheong 1996 Cheong, Fah-Chun. *Internet Agents: Spiders, Wanderers, Brokers, and Bots*. Indianapolis: New Riders Press, 1996.

Davis et al 2009 Davis, Michael, et al. *Hacking Exposed: Malware and Rootkits*. Emeryville: Osborne Publisher, 2009.

Deleuze and Guattari 1987 Deleuze, Gilles, and Felix Guattari. *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press, 1987.

Dyson 1997 Dyson, George B. *Darwin Among the Machines: The Evolution of Global Intelligence*. Reading: Addison-Wesley, 1997.

Falliere, Murchu, and Chien 2011 Falliere. *W32.Stuxnet Dossier*. *Symantec Security Response*. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ w32_stuxnet_dossier.pdf.

Gross 2011 Gross, Michael Joseph. “A Declaration of Cyber-War”. *Vanity Fair* (2011). http://www.vanityfair.com/culture/features/2011/04/stuxnet-2011104?

Hogland and Butler 2006 Hogland, Greg, and James Butler. *Rootkits: Subverting the Windows Kernel*. Upper Saddle River: Addison-Wesley, 2006.

Jackson 2008 Jackson, Devon. “Malware Wars”. *SFI Bulletin* 23 (2008).

Johnston 2008 Johnston, John. *The Allure of Machinic life: Cybernetics, Artificial Life, and the New AI*. Cambridge: MIT Press, 2009.

Johnston 2009 Johnston, John. “Mutant and Viral: Artificial Evolution and Software Ecology”. In Jussi Parikka and Tony Sampson, eds., *The Spam Book: On Viruses, Porn, and Other Anomalies From the Dark Side of Digital Culture*. Cresskill: Hampton Press, 2009.

Johnston 2010 Johnston, Casey. *Botnets Increasingly Wielded for Ideological Uses*. *Ars Technica*. 2010. http://arstechnica.com/security/news/2010/02/botnets-increasingly-wielded-for-ideological-uses.ars.

McMillan 2010 McMillan, Robert. *New Russian Botnet Tries to Kill Rival*. 2010. http://www.computerworld.com/s/article/9154618/New_Russian_botnet_tries_to_kill_rival.

Menn 2010 Menn, Joseph. *Fatal System Error*. New York: Public Affairs, 2010.

Mills 2010 Mills, Elenor. *Stuxnet: Fact vs. Theory*. 2010. http://news.cnet.com/8301-27080_3-20018530-245.html.

Obama 2009 Obama, Barack. *On Cybersecurity*. 2009. http://whitehouse.gov/video/President-Obama-on-Cybersecurity.

Parikka and Sampson 2009 Parikka, Jussi, and Tony Sampson, eds. *The Spam Book: On Viruses, Porn, and Other Anomalies From the Dark Side of Digital Culture*. Cresskill: Hampton Press, 2009.

Schiller et al 2007 Schiller, Craig, et al. *Botnets: The Killer Web App*. Syngress Press, 2007.

Suarez 2008 Suarez, Daniel. *Daemon*. New York: Dutton, 2008.

Suarez 2008b Suarez, Daniel. *Bot-Mediated Reality*. 2008. http://fora.tv/2008/08/08/Daniel_Suarez_Daemon_Bot-Mediated.

Suarez 2010 Suarez, Daniel. *Freedom*. New York: Dutton, 2010.