Chapter 20
The Case of the U.S. Mother / Cyberspy / Undercover Iraqi Militant:
Or, how Global Women Have Been Incorporated in the Technological War on Terror

Winifred R. Poster[1]
Washington University, USA

ABSTRACT

While literatures on women in technology and women in the military are well-developed, the field of cybersecurity has yet to be addressed within either of them. Therefore, this analysis charts a typology of work in global ICTs, an "information hierarchy," and explores the presence and contributions of women at multiple levels. It identifies selected jobs for women in cybersecurity as illustrations of these dynamics. This starts with "networkers" at the top: the infoczars who lead the nation's agencies for military and information security, and engineers who design the military technology systems. In the middle "networked" level, this includes cyber spies (posing from their homes as Al Qaeda militants on the internet) and customer service workers (enforcing US homeland security on the phone with the public). At the bottom, it includes "switched off" workers: flight attendants and transit screeners, who use security information embedded in computers for the surveillance of people's bodies. This chapter takes focus on the middle level of the hierarchy in particular. The discussion considers the transformations women make in this field, as well as their political tradeoffs in supporting US political campaigns in the Global South.

DOI: 10.4018/978-1-4666-0020-1.ch020

INTRODUCTION

Women are not thought of very often when it comes to the front lines of cyber security and the war on terror. However, women are playing key roles in a variety of different settings where they use advanced technical equipment and sometimes risk their lives. These women may not be the instigators or chiefs of the war on terror, but they are often responsible for carrying out the everyday tasks which support the U.S. administration's campaigns.

Shannen Rossmiller, as a prime example, is the homemaker-cyberspy who has become one of the FBI's first and most accomplished cyber counter-terrorists. She is just one sign of underlying shifts in the global economy which have opened doors for women in the work of security and military technology. Cybersecurity is the new field that has been generated by a convergence of spheres: the integration of information technology into the military, and the diffusion of militarism throughout the information society. With this process, the work of fighting "terrorists" is done in everyday life – especially where women are. It is done in transportation, service industries, and even people's homes. This process has also been transnational, as US women interact online with political actors in the Middle East, and as the outsourcing of ICT work incorporates women in the Global South in security campaigns for the Global North. As a networked employee in the information hierarchy, Rossmiller represents women's agency in using the virtual to participate in counter-intelligence work.

LITERATURE REVIEW

The Dawn of Cybersecurity

War is going cyber. ICTs are being integrated into many aspects of military staging (Latham 2003; Osler and Hollis 2001). This encompasses a wide range of activities, from the use of physical military force to control media and communication outlets, to the manipulation of information for war propaganda, to the infiltration of online networks and databases for the purposes of disruption or theft, and the use of ICTs to coordinate political actors who are geographically dispersed.

In the US context, the technology agenda has had a long history in military institutions. However, several circumstances have changed its path and vigor in the twenty-first century.

First is the sudden expansion of the ICT sector through the internet, satellite and mobile phone communications, and computer technology. Second is 9/11, an era which ushered in a heightened military drive by the US administration in its war on terror. Third is the Obama administration which has favored science and technology as key features of governance, unlike its predecessors. Just in time: attempts to infiltrate government's networks have multiplied exponentially in the last few years, with thousands of episodes a day. In turn, there is a "heightened awareness across the military that it must treat the threat of a computer attack as seriously as it does an attack carried by a bomber or combat brigade. There is hardly an American military unit or headquarters that has not been ordered to analyze the risk of cyberattacks to its mission – and to train to counter them" (Kilgannon and Cohen 2009, A14).

Cybersecurity is the military's response to cyberwar. It involves using technology to protect military activities and installations, and the use of the military to protect information and data. While the term is often used in a limited sense to describe the act of securing of online data, I use it in a much broader manner to describe the variety of ways in which militarism, security, information, and technology are intertwined in the configuration of new jobs. I'll return to this later, but first let me turn to the issue of gender.

The Curious Draw of Women to Cybersecurity

The gendering of cybersecurity is quite a puzzle. As this analysis will illustrate, there has been a dramatic pull of women into the new positions of cybersecurity. Yet, both of the fields from which cybersecurity has originated are egregiously lacking in women.

Take IT industries to start with. Even though women comprise 57% of the workforce in the US, they occupy only 25% of professional level IT jobs. Among the Fortune 500 technology companies, women hold 11% of the leadership (corporate officer) positions. This trend, moreover, has been downward. Rates of women in IT educational degree programs and careers have been falling, even when they were low to begin with. Over the last decade alone, college women's interest in majoring in computer science has declined by almost 60%. Bachelors' degrees in computer and information science among women have dropped 37% between 1985 and 2008. And while the percentage of women in computer-related occupations was at its peak in 1991 at 36%, this has dropped 12 percentage points since then to 24% in 2008 (Ashcraft and Blithe 2010; National Center for Women & Information Technology 2010).

The story is not much brighter in the military. Women are still vastly under-represented in US armed forces. They make up on average 14% of those in active duty, at 208,000. Their numbers are greatest in the air force (20%) and lowest in the marines (6%). In leadership, women represent 7% of the Admirals, and 16% of the Officers. Of all four branches of the military, only one woman holds the highest post of General-Admiral from a total of 41. (Data are from 2009, Institute for Women's Leadership, 2010; Women in Military Service for America Memorial Foundation, 2010).

Several questions arise then: what draws women to cybersecurity, and cybersecurity to women? How have women been able to make inroads in this field when their progress has been so difficult in information technology and in the military alone?

The answers, I will argue, are not easily found in the existing literatures on women in either the military or technology. Feminist scholars of ICTs have documented the formidable and ascending barriers for women in computing. It starts from early childhood socialization away from technology, to segregated educational systems, and then on to hostile environments in the IT workplace (sometimes called "masculine cultures of engineering") where technical prowess is linked to masculinity (Cockburn 1985; Cohoon and Aspray 2006; Margolis and Fisher 2002; McIlwee and Robinson 1992). However, this field has been primarily interested in women engineers in IT firms, and has yet to delve into the realm of women in the military or who work with military technology (exceptions to be discussed below).

The feminist literature on the military faces the opposite issue – ignoring the information era. There is ample research on the gendering of militarism, and the hostile nature of the military institutions to women. This literature describes explicit governmental regulations prohibiting women from certain military tasks, as well as more informal practices and symbols which devalue women and femininity. Yet, most of the studies have been limited to traditional roles and issues of the pre-information era (i.e., whether women should be in combat situations, in close quarters with men, etc.). From either viewpoint then, one is not seeing the vast new areas of women's participation in militarism: as IT leaders, as developers, and practitioners.

A better understanding of women in cybersecurity, I will argue, lies in seeing these spheres as dynamically inter-related rather than separate. First, there is an integration of ICTs into the military. The job of militarism is shifting in the information age. Daily activities are occurring at computers in offices rather than just in the field with guns. The tasks are becoming technical rather than just physical. The bodies needed for these

jobs are increasingly mental and gender-neutral, and less linked only to brute force strength and masculinity. In short, cybersecurity involves new ICT skills – ones which women tend to be drawn to and excel at.

The second trend is the reverse: an integration of militarism into the information economy, largely through technology. With this process, the work of fighting "terrorists" is done in everyday life – especially where women are. It is done in transportation, service industries, and even people's homes. I will show how, while each of these fields repels women on their own, their recent merging has created a formulative mix that has made them more inclusive.

Cybersecurity Jobs and the Information Hierarchy

Cybersecurity involves a wide range of jobs with different capacities of technology, levels of authority and skill, and gender compositions. In order to get an idea of how these dimensions are structured, I turn to the literature on ICTs in labor and elaborate a framework for military jobs in particular (Table 1).

As a starting point for understanding how ICT work is defined and organized, I borrow from what Castells (2000) has described as a "network" relation. Individuals who work and interact through the internet, satellite phones, etc., have different capacities "to link up with other workers in real time" (p. 260). These individuals are grouped on a scale, from "the networkers, who set up connections on their initiative... and navigate the routes of the network enterprise; the networked, workers who are on-line but without deciding when, how, why, or with whom; the switched-off workers, tied to their own specific tasks, defined by non-interactive, one-way instructions."

From this perspective, the ability of workers to access the network is central to the conceptualization. The most privileged workers are not only able to connect to the internet, but they are responsible for developing the network infrastructure itself. Mid-level workers are the subsequent users – those who navigate it on a daily basis (participating in collective forums, communicating with others, joining virtual worlds, etc.). Marginalized workers are excluded from the network altogether (even though still using technology), or else they relate to the network very sparingly, by transferring information in a singular path (e.g., downloading documents) and without communicating to others.

Employees also vary in their tools for connecting to the network and doing ICT work (Montagnier and van Welsum 2006). High level workers have a wide spectrum of hardware and software at their disposal as they develop and

Table 1. The information hierarchy of cybersecurity work

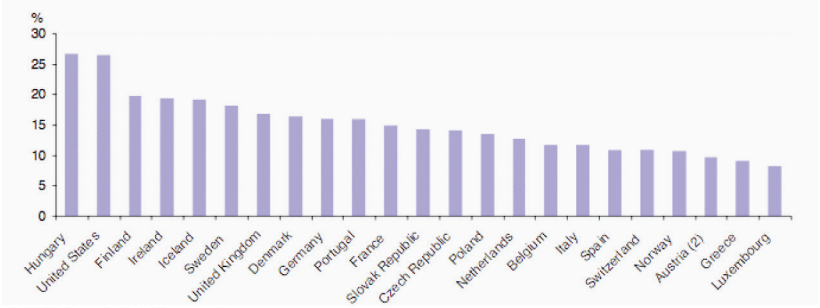
		Level of Hierarchy	
Feature of Work	Networker	Networked	Switched Off
Relation to Internet	Sets Connections Designs Virtual Spaces	Online Interactive	Offline Non-interactive
Relation to ICTs (Hardware and Software)	Developer Maintainer	User of Advanced or Specialized ICTs	User of Basic ICTs
Female Composition	Low	Variable	High
Representative Cybersecurity Jobs	Info-Czar Security Engineer	CyberSpy Call Center Worker	Flight Attendant Transit Screener

Note: This framework integrates and elaborates conceptualizations from Castells (2000) and Montagnier and van Welsum (2006). Responsibility for the final form is my own.

maintain ICT systems. Mid level workers often have access to specialized types of software and hardware, especially for their particular sector. Low level workers have access to at best basic software and other simple hardware technologies.

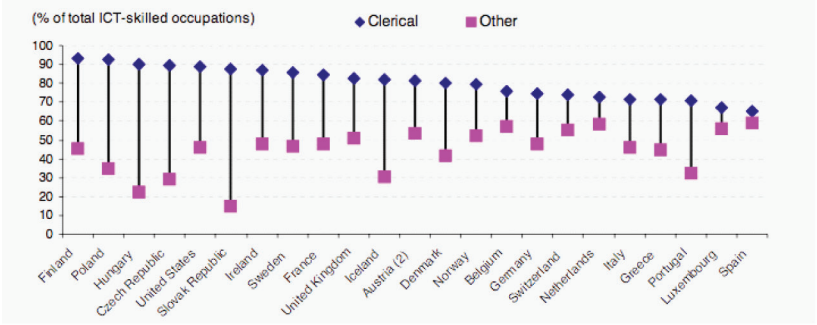
Women's presence in these jobs decreases going up the hierarchy. Figure 1 provides data on women's shares of ICT jobs from the US and Europe for 2004. Women occupy a small percentage (10-25%) of the highest level "ICT-Specialist" occupations (like web developers, system programmers, database administrators, telecommunications and hardware engineers, IT consultants, etc.). They are better represented (30-50%) in the mid-range "ICT-Using" occupations, in which employees utilitze a broad range of sector-specific or else generic software for their jobs. Not surprisingly, women are over-concentrated at the bottom of the scale, making up 60-95% of the "ICT-Clerical" occupations (like secretaries, keyboard operators, information clerks, administrative assistants, etc.). These workers are limited to data and word processing

Figure 1. Share of women in ICT occupations, US and Europe, 2004. Source: OECD (Montagnier and van Welsom, 2006, pp. 11-13)



a) ICT-Specialist Occupations

b) ICT-Using Occupations



c) Clerical (vs. Other) ICT-Using Occupations

programs like Microsoft word, powerpoint, excel, outlook, etc., in their daily routines.

Jobs in the middle category vary in their gender composition, however. In telecommunications work (Table 2), for instance, women far outnumber men in countries like Azerbaijan, Kyrgyzstan, Romania, Gambia, Cape Verde, and Cuba, where their shares reach well above 50-80% in some cases. Women's shares fall below 15% in selected countries of the Middle East and Africa, like the United Arab Emirates, Qatar, Iran, Saudi Arabia, Malawi, Yemen, Benin, and Burkina Faso. World averages for women in telecommunications are around 30% (International Telecommunications Union 2001).

Within each of these core levels of the information hierarchy are many cybersecurity positions. As illustrations, I identify selected jobs that are representative of women's roles. This starts with "networkers" at the top: the women infoczars who lead the nation's agencies for military and information security, and engineers who design the military technology systems. In the middle "networked" level, this includes women cyber spies (posing from their homes as Al Qaeda militants on the internet) and customer service workers (enforcing US homeland security on the phone with the public). At the bottom, it includes "switched off" workers: women flight attendants and transit screeners, who use security information embedded in computers for the surveillance of people's bodies.

My larger project considers each of these jobs in detail, and the unique ways that they impact women in cybersecurity. For this chapter, I focus on the middle level of the hierarchy in particular. As a networked employee in the information hierarchy, Rossmiller represents women's agency in using the virtual to participate in counter-intelligence work.

This analysis draws from original research in the US. I have conducted interviews in person and over the phone with women and men in cybersecurity roles. These are independent workers and founders of private security and research firms, some of whom contract with military or government organizations. I've also examined a variety of their professional materials including their websites, surveillance monitoring cameras, research publications, and powerpoint presentations.

To follow policies and practice of the US state, I examined original documents and websites concerning cyberwar and women in ICT jobs. These are from military and government offices like the Defense Advanced Research Program Agency, the Transportation Security Administration and their employee unions, the US House of Representatives, etc. I gathered statistical data on women's participation in ICT and military occupations globally from a range of state, inter-governmental, and non-governmental sources: the Bureau of Labor Statistics, International Telecommunication Union, International Labour Organization, the Organization of Economic and Development Cooperation, the National Center for Women &

Figure 2. Cyberspy Shannen Rossmiller, working in her kitchen; one of her virtual alter egos, Abu Zeida. Source: Colbert (2010); Rossmiller (2008)

Table 2. Female telecommunications staff globally, 2001, by descending percent

Country	Total	% Female
Azerbaijan	7,040	80%
S. Tomé & Principe	84	78%
Gambia	723	75%
Cape Verde	312	67%
Kyrgyzstan	4,103	53%
Romania	20,761	52%
Cuba	8,453	51%
Eritrea	243	51%
Marshall Islands	52	50%
Armenia	3,392	47%
Kiribati	69	44%
Barbados	448	43%
Myanmar	3,431	43%
Latvia	1,657	41%
Moldova	2,894	40%
Czech Republic	9,585	39%
Lesotho	134	38%
Sweden	9,752	38%
Albania	1,364	37%
Tonga	110	37%
Macao	428	35%
Slovak Republic	5,178	35%
Ethiopia	2,502	34%
Grenada	91	34%
Guinea	265	33%
Seychelles	123	33%
Taiwan	14,341	33%
Slovenia	1,286	31%
Tanzania	1,066	30%
Tunisia	2,229	30%
Lao P,D.R	389	29%
Botswana	489	28%
Guernsey	79	28%
Kenya	5,388	28%
Suriname	282	28%
Syria	5,856	27%
Angola	547	26%
United Kingdom	53,300	25%
Cyprus	589	24%
Ecuador	1,160	24%
Maldives	127	24%
Senegal	366	24%
Côte d'Ivoire	883	23%
Zambia	714	23%
Egypt	12,059	22%
Madagascar	553	22%
Mali	305	22%
South Africa	10,224	22%
Bosnia	367	20%
Jordan	1,285	20%
Mauritius	372	20%
Micronesia	27	20%
Sri Lanka	2,289	20%
St. Vincent	33	20%
Ghana	763	19%
Papua New Guinea	340	19%
Greece	3,394	18%
Sudan	542	18%
Togo	161	18%
Nigeria	1,012	17%
Turkey	11,319	16%
Solomon Islands	22	15%
Central African Rep.	58	14%
United Arab Emirates	1,236	14%
Benin	157	13%
Burkina Faso	165	13%
Qatar	222	13%
Bhutan	40	11%
Malawi	312	10%
Yemen	387	7%
Iran	3,063	6%
Saudi Arabia	-	0%

Source: International Telecommunication Union (2001)

Information Technology, the Women in Military Service Foundation, etc.

Networked Women: US Cyber Spies

In perhaps the most unexpected way, ICTs are opening roles for women in the heart of intelligence as cyber spies. Shannen Rossmiller is a Montana farmer's daughter and mother of three who has become one of the FBI's – first and possibly most accomplished – cyber counter-terrorists. Sitting at her kitchen computer, while her children were sleeping or getting ready for school, she has infiltrated online extremist chat rooms posing as various male Islamic militants. A "networked employee," Rossmiller's story shows how women are participating in the new realm of military strategizing online.

Rossmiller ended up in cyber security through a circuitous path. After studying criminology in college, she worked as a paralegal and eventually became a municipal judge (the youngest woman in the country to do so, at the age of 29). After 9/11, she took it upon herself to do something about the Al Qaeda threat. She made a very poignant observation about the role of technology in contemporary warfare: "how extensively Al-Qaeda used the Internet to orchestrate 9-11 and how out of touch our intelligence agencies were regarding this internet activity. Apparently, there were not procedures in place for tracking communications and activity on the Al-Qaeda websites and Internet forums at the time" (Rossmiller 2007, p. 1).

In 2002, she started to peruse Arab political websites and community forums like www.alneda.com, alfirdaws.org, arabforum.net, the Paradise Jihadist Supporters Forum, and Yahoo chat groups "bravemuslims," etc. She learned, partly through trial and error, that this context could be very effective for acquiring information on potential security breaches and catching terrorists in the planning stages of violent acts. But what she does is more than just collect data. She created an entire strategy of counter-intelligence work on her own, independent of the military, which then became a core asset of espionage in the information age.

Three strategies in particular illustrate how a woman at home in Montana can use ICTs to defeat militants half way across the world. The first is intense cross-cultural self-training through technology. Prior to 9/11, Rossmiller had no background at all in Middle Eastern societies or language. She discovered, however, that ICTs offer many ways to catch up in a short amount of time and without leaving her house. She taught herself Arabic by taking online courses with e-schools like the Arab Academy in Cairo. She used Google text translator and an online translation service to understand other peoples' posts. She used the internet to research the precise area her character was from, so that she could comment on neighborhood restaurants, mosques, or imams. She watched foreign news programs on cable television to learn up-to-date local events and put them in her communications. She read over 50 books on the Middle East, including the Koran, from which she collected quotes and stories. Inserting lines from Arabic poetry in her emails would be a very helpful way to garner trust, she discovered.

Taking the cultural immersion one step further, Rossmiller took the persona of a Middle Easterner by practicing national identity management: "I learned to act like them... I learned to be like them" (Hayasaki 2009, p. 1). There are many aliases in her repertoire: she has posed as an Iraqi courier, a jihadist banker, an Algerian Al Qaeda operative and a recruiter. She develops full identities for her alter egos, keeping files on her computer with their date of birth, city where they are from, a biosketch, and photos from the internet (Colbert 2010). Some are older and rural looking, like Abu Abdullah, who has a beard and head scarf. Others are young, hip, and urban like Abu Musa and Abu al Haqq, who are clean-shaven, and don sportswear and glasses. She becomes emotionally invested in the characters. She cries when they "die" – killing or martyring them off when they are no longer useful. (In the future, she will undoubtedly have

personas from other global regions. She is now learning Chinese and Russian so she can start to shift her tactics to those cybersecurity threats, as have occurred more recently).

Rossmiller's personal features and background couldn't be further from those she portrays in cyperspace. She is white, middle class, middle-aged, with blond hair. She was on the cheerleading squad in high school, was voted miss congeniality, and lives in a small town the midwest. She has two school-aged kids and one in college. She notes that many, if not most, of the people with whom she interacts on a daily basis would be shocked by knowing her real identity. This includes the men in the Middle East with whom she chats online: "If they could see me, little blond me, they'd go crazy" (Hitt 2007, p. 264). But it also includes the male staff at the FBI, to whom she was initially hesitant to meet in person for fear of not being taken seriously as a woman. Indeed, her real identity would likely be obstructive to her goals with both with her enemies and her colleagues. Altering her identity, then, had practical uses in many global and local contexts.

A second tool that Rossmiller uses is social engineering. This is a communicative skill, operating entirely through ICTs, for manipulating people and building allegiances. Indeed, from a military standpoint, the communicative strategy of "chatting" is key for intelligence surveillance in the information age. However, what Rossmiller does is not just simple conversation. It is a sophisticated and subtle tactic of interpersonal relations. She figured out early on that niceness and friendliness will not garner trust from this group. Rather, being a bully (i.e., masculine) is much more effective. Not overly aggressive, but definitely pushy, dismissive, and arrogant. If she wants an invitation to a chatroom, she uses a "demanding tone" (Hitt, p. 264). She has also keenly mastered the use of Islamic social practices. To get targets to divulge private information, she asks them to fill out and email her an "Oath of Allegiance" or bayat, in which they disclose their addresses, locations, etc.

A third strategy for Rossmiller is equipping herself with simple yet powerful spy technology. She set her home up with typical consumer hardware (albeit multiplied): eight PCs, two servers, and two broadband lines. She uses software tools that are shockingly common and accessible on the internet. Search engines, for instance, enable her to look up the names, pictures, and email addresses of the chatroom contacts, as well their IP addresses and locations. Other technologies are more sophisticated and more hacker-ish. She installs a proxy server on her computer yielding a fake IP address, so that no one can trace her own location. She uses a "keylogger" to record every keystroke that her target is making. Hidden in something like a picture and then sent within an email message, the keylogger remits important information (like a password) typed by the recipient.

Rossmiller also combines low and high technologies. She uses old-fashioned note-taking to keep meticulous files about the 600+ people with whom she has communicated. With digital programs, she records her online activities with time-stamps and screen shots. Subsequently, she uses her computer to store and retrieve the information, a practice of databasing (Poster 2011). Her most advanced technical tools involve computer engineering. With a colleague who is a nuclear physicist, she learned programming so that she could break code and unencrypt email messages from the Global Islamic Media Front.

Finally, Rossmiller's location has yielded her many advantages. Working almost entirely inside her home, she has gained autonomy and agility to develop these cyber-sleuthing practices. For one thing, it enables her to bypass the loaded bureaucracy and underdeveloped technology of government intelligence work. Ironically, the relatively common technologies in her household were more advanced than those of the local FBI. She was shocked that some of her counterparts in the FBI face mammoth hurdles to carry out

routine tasks: needing permission before opening a Yahoo account; having to go to the public library in order to surf the internet, etc. In this way, the mass availability of consumer electronics, the downloadability of software, and the globally-connected spaces of the internet allowed her to assemble all the tools she needs.

There are other practical benefits of working at home. Rossmiller can conduct 24-hour tracking of her targets. She can correspond live with peers in chatrooms across time zones (which means sitting at the laptop between 3am and sunrise). Indeed, such reversals of work time are becoming typical features of employment in the global economy (Poster 2007). From a gender point of view, there are additional advantages. The home provides refuge from a masculine environment of the FBI, which at least in the beginning was dismissive of and intimidated by her. She describes the government in general as "a man's world," which is one reason why she doesn't want to work there. And then there is her family. Through home-based work, she does her mothering and cyberspy duties at the same time. Of course, working at home has many costs too, not the least of which are being alienated from colleagues, cut off from organizational resources, and prone to overwork. For spies, there are job-specific dangers on top of this. She has received many death threats. Her car was stolen from her own garage, and later found full of bullet holes. Her home was broken into, and she had to find a new place to live for her family (Hayasaki 2009).

Still, Rossmiller is committed to her domestic work location. Even though she set up her own cybersecurity firm in 2008, she still works at home part time. Her independent location, both geographically and institutionally, enables her the freedom to experiment with technology and with strategy. As one journalist observes, the FBI "can't even *begin* to match what Rossmiller does" (Hitt, p. 262). She says she is able to "think outside of the box" and "outthink and outmaneuver the terror army …by forging new and untested methods in the field of cyber-counterintelligence," (Rossmiller, p. 4). When I asked her if she ever wanted to work directly for the FBI, she said emphatically no. In this way, the expansion of ICTs into the household has provided women with an opportunity to engage in militarism through non-traditional sites.

By her own account, she has had many successes from this work ("actionable intelligence" and "enemy captures" in military lingo). Since 9/11, she has exposed weapon caches, bomb plots, and cells in over 200 operations which she handed to the FBI and Department of Homeland Security. Although most of her foreign operations are classified, some of her domestic activities have been very high profile. For instance, she helped to convict two US citizens who were appearing on her insurgent websites. They were trying to collaborate with Al Qaeda, plot bombings, and commit espionage in the US. She claims that her sleuthing tactics would "become a template for the government in the new and developing field of fighting terrorism online" (Rossmiller, 2007, p. 4).

In her latest endeavor, Rossmiller is developing new technologies that will help others conduct cyberspy work. Largely out of frustration with the existing FBI technology and its failure to account for cross-cultural differences, she is currently working on a software program called ASYLMM (Rossmiller 2010b). It has a "mindset filter" which is a computerized means of "understanding the enemy by finding indicators of hidden radicalization on the web and teaching an individual how to think like the Middle Eastern world" (Rossmiller 2010a). It assembles a vast collection of detailed information about Afghanistan (as one location) from her own database as well as from newly acquired intelligence in newspapers, voice recordings, etc. Not only will this program help operatives don the personas of militants as she does, it will also help them to understand how the militant is viewing them (Rossmiller 2010b, p. 1):

Implicit within the mindsets of the observer and the subject are the cultural, religious, and ideological

biases of each. Rather than eliminate these effects, we seek to account for them over the course of the interaction, thereby effectively allowing the observer to view the interaction from within the mindset of the subject while taking her[2] own mindset into account.

The idea is to prepare military personnel to avoid miscommunications and be mindful of subtle cues, such as the way some Middle Easterners use greetings to indicate whether or not they are a religious fundamentalist. Thus, her emphasis on integrating a cultural filter in the data mining process shows her sensitivity to global understanding – both a deep attention to the politicization within layers upon layers of interactions (i.e., how they view us, how they view us viewing them, etc.) and a drive to inscribe this transnational awareness into software code.

DISCUSSION

Rossmiller's case offers a poignant illustration of how the merging of militarization with the information society is generating sites for women's agency in cybersecurity. On one hand, selected political activities by Iraqi and Afghani militants have moved to the internet (chatrooms, forums, etc.), transferring the location for intelligence work online as well. On the other hand, the movement of ICTs to the household, and the connections they provide globally, mean that women can participate in those military strategies without traveling there physically or being formally integrated in military institutions.

As a "networked" employee in the information hierarchy, Rossmiller represents several ways that women can have agency in using the virtual to participate in counter-intelligence work. First, she has used ICTs to gain access to military playing fields virtually, even when she may be restricted from such military activities on the ground. She has cleverly assembled an array of ICT resources to overcome structural limitations and take up this new field task despite her background in an entirely different area. With few institutional supports or resources (financial, organizational, informational, or otherwise), without a large scale team, without prior knowledge of Middle East politics or ever traveling there, *without any training in counter-intelligence or military tactics*, and in addition, and *without any background in engineering or technology*, she was able to forge a career in cybersecurity. This suggests that ICTs can provide a unique platform for a woman to develop military skills.

Second, she has used the online platform to alter her gender and nationality in cybersecurity work, and moreover, she has enacted militarized personas that are radically different from her own. In some ways, this has happened before. Intelligence operatives often engage in role playing. And from a gender point of view, women have been passing as men in order to join in armies as soldiers for hundreds of years (Peterson and Runyan 2010), the most famous perhaps being Joan of Arc.

However, with the arrival of the internet, this cyber-spy work can be done without the actual body involved. This frees the spy from the task of maintaining the physical appearance for the role. In exchange, it forces him/her to be hypervigilant about the interactional presentation of self. Every word and tone used in conversation may be highly scrutinized for authenticity. It is this high level of detail in communicative labor that Rossmiller has excelled at. Furthermore, she has been better at acting as an Iraqi militant than many of her male counterparts in the FBI. This raises questions as to whether US women are more skilled cyberwarriors than men, or at least, better at acting out the military masculinities of the Global South.

This brings us to the third point: Rossmiller's work is indicative of the "hybrid skills" (Woodfield 2000) that women bring to cybersecurity: she is adept at both the technical aspects of online in-

telligence gathering through ICTs, and the social aspects of communication and interaction in virtual forums. She is both an actor and an engineer. Offering a global perspective to Woodfield's concept, I would add that women cybersecurity workers are also interjecting a transnational dimension to these hybrid skills. Not only are they fusing the social and technical, they are placing this in transnational context, using ICTs to integrate cross-cultural practices in intelligence technologies. And, as a designer of new military technology for this end, she is now traversing the line between networked and networker, and moving up the tiers of the information hierarchy.

Finally, what marks Rossmiller's story is her role as one of the first occupants in this field. She is not just the first *woman* in this job of cyberspy; she is one of the *first* cyberspies ever. Just as with several other cases in the information hierarchy (e.g. the info-czars), women are being placed in, and / or are charting, the newest fields of military information. So while she may be not be a "typical" woman in the military right now, she is a pathbreaker and perhaps will be followed by more women in the future.

CONCLUSION

Women in the US are becoming the figureheads, designers, and practitioners of counter-intelligence and military ICT strategy, as well the enforcers of military security on the ground and online. They are forming an information hierarchy of cybersecurity work, which I chart in fuller detail in a larger project. Here, I have argued that women's surprising entrance in these key jobs of the twenty-first century is grounded in a dual process: the integration of information technology into the military, and the diffusion of militarism throughout the information society.

While women in the Global North seem to breaking ICT barriers through cybersecurity, the political implications are less clear. Namely, are the benefits for women from forging ICTs careers overshadowed by their contributions to the war on terror campaigns? Global feminist scholars argue these policies are harmful to women in Iraq and Afghanistan, both materially, through funding cuts to women's international programs, and symbolically, by silencing those women and presenting them in the media as victims (Agathangelou and Ling 2004; Nayak 2006; Youngs 2006). Therefore, if Rossmiller is passing on information to the US government to use in its own ways, one might argue that her activities are by default supporting these campaigns, even if indirectly. Rossmiller does have critiques of the Bush administration (in making Iraqi militants angry unnecessarily). Still, she is highly nationalistic, inserting extensive patriotic rhetoric and symbolism (e.g., images of Bush, the statue of liberty, etc.) in her lecture materials.

The alternative is that the women reviewed here are shifting policies, strategies, and narratives of militarism for the US government through their cybersecurity work. Rossmiller certainly believes that this is the case. She describes how the existing paradigm of counter-intelligence is dangerous (Rossmiller 2010b, p. 1):

... the significance of this problem cannot be overstated. The cost in terms of lives and treasure expended in the course of foreign operations is huge in numbers and in the effect upon morale, both civilian and military. Many times, this cost is increased simply because we do not bother to study the minds of the enemy or others in the theater whose roles have a direct or indirect impact on the outcome of these operations.

She sees her methods of cyber-investigation as far more sensitive to local populations and averting of undue harm. In either case, future research should explore whether the ICT gains for women in the North are coming at the expense of women in the South.

Certainly, this story can be told with a complementary view of women in the Global South, who are using ICTs to advance their interests as well. For instance, RAWA, the Revolutionary Association of the Women of Afghanistan, has been using website activism to develop NGOs and organize internationally when not allowed to do so locally under the Taliban (Dartnell 2003). Indeed, the role of women in political and military technologies is transnational and deserving of more attention.

REFERENCES

Agathangelou, A. M., & Ling, L. H. M. (2004). Power, borders, security, wealth. *International Studies Quarterly*, *48*, 517–538. doi:10.1111/j.0020-8833.2004.00313.x

Ashcraft, C., & Blithe, S. (2010). *Women in IT: The facts*. Boulder, CO: National Center for Women & Information Technology.

Cockburn, C. (1985). *Machinery of dominance: Women, men and technical know-how*. London, UK: Pluto Press.

Cohoon, J. M., & Aspray, W. (2006). *Women and Information Technology*. Cambridge, MA: MIT Press.

Colbert, T. (2010). *Powerpoint presentation: Manuevering the media minefield*. CA: Camarillo.

Dartnell, M. (2003). Information Technology and the Web activism of the Revolutionary Association of the Women of Afghanistan (RAWA). In Latham, R. (Ed.), *Bombs and bandwidth* (pp. 251–267). New York, NY: The New Press.

Hayasaki, E. (2009, January 11). Cyber-spy shares her know-how tracking terrorists. *Los Angeles Times*.

Hitt, J. (2007). I spy. *Wired*, 244-264.

International Telecommunications Union. (2001). *Female telecommunications staff*.

Kilgannon, C., & Cohen, N. (2009, May 11). Cadets trade the trenches for firewalls. *New York Times*, A1, A14.

Latham, R. (2003). *Bombs and bandwidth*. New York, NY: The New Press.

Margolis, J., & Fisher, A. (2002). *Unlocking the clubhouse: Women in computing*. Cambridge, MA: MIT Press.

McIlwee, J., & Robinson, J. G. (1992). *Women in engineering: Gender, power, and workplace culture*. Albany, NY: State University of New York Press.

Montagnier, P., & van Welsum, D. (2006). *ICTs and gender: Evidence from OECD and non-OECD countries*, (pp. 1-46). Organisation for Economic Cooperation and Development. Retrieved July 27, 2010, from www.oecd.org

National Center for Women & Information Technology. (2010). *By the numbers 2009*. Retrieved July 9, 2010, from www.ncwit.org

Nayak, M. (2006). Orientalism and "saving" US state identity after 9/11. *International Feminist Journal of Politics*, *8*(1), 42–61. doi:10.1080/14616740500415458

Osler, F., & Hollis, P. (2001). *Activists guide to the Internet*. London, UK: Prentice Hall.

Peterson, V. S., & Runyan, A. S. (2010). *Global gender issues in the new millenium*. Boulder, CO: Westview Press.

Poster, W.R. (2007). Saying "good morning" in the night: The reversal of work time in global ICT service work. In Rubin, B. (Ed.), *Research in the sociology of work* (*Vol. 17*, pp. 55–112). Amserdam, The Netherlands: Elsevier.

Poster, W.R. (2011). Emotion detectors, answering machines and e-unions: Multisurveillances in the global interactive services industry. *The American Behavioral Scientist*, *55*(7). doi:10.1177/0002764211407833

Rossmiller, S. (2007). My cyber counter-jihad. *Middle East Quarterly*, (Summer): 43–48.

Rossmiler, S. (2008). *Penetrating minds of mayhem: Inside the mind of an Islamic extremist*. Powerpoint Presentation: AC-CIO, LLC Intel Ops.

Rossmiller, S. (2010a). *Personal interview* (April 27).

Rossmiller, S. (2010b). *ASYLUMM: A situational diagnostic tool*. Helena, MT: Advanced Cyber-Counter Intelligence Operations, LLC.

Woodfield, R. (2000). *Women, work, and computing*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511488948

Youngs, G. (2006). Feminist international relations in the age of the War on Terror. *International Feminist Journal of Politics*, *8*(1), 3–18. doi:10.1080/14616740500415409

ENDNOTE

1 Many thanks to the editors of this volume, to Carol Needham and Amy Wilhelm for their comments, and to Shannen Rossmiller for offering her time and her story for this analysis. All opinions expressed herein are my own.

2 Note the female pronoun here: with alternating gender pronouns in her report, she expects new recruits to be female as well as male.