

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. Poster¹
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 infocars 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.

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/case-mother-cyberspy-undercover-iraqi/62890

Related Content

A Rule-Based Quality Analytics System for the Global Wine Industry

Carmen K. H. Lee, Kris M. Y. Law and Andrew W. H. Ip (2021). *Journal of Global Information Management* (pp. 1-18).

www.irma-international.org/article/a-rule-based-quality-analytics-system-for-the-global-wine-industry/255847

Expense and Exposure: Virtual Global Education for Tomorrow

Bobbe Cummins Colburn and Julie Nolin (2012). *Disruptive Technologies, Innovation and Global Redesign: Emerging Implications* (pp. 395-406).

www.irma-international.org/chapter/expense-exposure-virtual-global-education/63842

Absorptive Capacity and ERP Implementation in Indian Medium-Sized Firms

Seema Sharma, Elizabeth M. Daniel and Colin Gray (2012). *Journal of Global Information Management* (pp. 54-79).

www.irma-international.org/article/absorptive-capacity-erp-implementation-indian/70665

Ethics and Social Responsibility for 21st Century ICT

Duane Windsor (2025). *Encyclopedia of Information Science and Technology, Sixth Edition* (pp. 1-14).

www.irma-international.org/chapter/ethics-and-social-responsibility-for-21st-century-ict/342842

Thinking About Globalization as an Integration Process

Jen Ma and Hugh Dang (2023). *Journal of Global Information Management* (pp. 1-14).

www.irma-international.org/article/thinking-about-globalization-as-an-integration-process/321175