COMMENT

DAVID HOWELLS/CORBIS/GETTY

Cyberspy Shannen Rossmiller posed as male Iraqi and Afghan militants in extremist chat rooms to expose weapon caches and bomb plots.

Cybersecurity needs women

Safeguarding our lives online requires skills and experiences that lie beyond masculine stereotypes of the hacker and soldier, says **Winifred R. Poster**.

Computer hacking is becoming more widespread and damaging. Headlines highlight attacks on government agencies, political campaign offices, financial institutions and big corporations. But citizens and consumers are paying a heavy price. In 2016, 2 billion people had their personal details stolen, including the medical records of more than 100 million Americans. Hacks of US retail outlets such as Target and global credit companies such as Equifax compromised the private data of hundreds of millions of customers. In the past 6 years, more than US$107 billion was stolen from US consumers through identity theft.

Cybercrime exacerbates inequalities. A million more US women than men had their identities stolen in 2014. People of African American and Latino descent are, on average, two to three times more likely than white people to be victims of fraud related to debt or income. And women and girls are more likely than men to be targets of 'remote sexual abuse' — coerced into posing nude online or being stalked through the Internet.

Security technologies also disadvantage women and other groups. For example, biometric facial recognition systems have trouble identifying the faces of women and people of colour. Airport security systems and operators disproportionately flag black women for strip searches relative to other passengers[1].

Cybersecurity professionals — who protect databases, software systems and computer networks from access, change or destruction — are predominantly male. Women comprise only 11% of these professionals worldwide, and only 14% in North America (see 'Women in cybersecurity'). By comparison, women make up 57% of the US professional workforce. Even cybersecurity's sister industries do better: 15% of the US military and 25% of staff in information technology are women (see 'Sister fields'). By 2020, 2 million more cybersecurity jobs will be needed worldwide in addition to the 3.2 million people who are already ▶

employed in the field, of whom almost 750,000 are in the United States.

Cybersecurity's future depends on its ability to attract, retain and promote women, who represent a highly skilled and under-tapped resource. The discipline also needs to learn about women's experiences as victims of cybercrime and the steps needed to address the imbalance of harm.

Here I highlight four ways in which the field should adapt.

FOUR PRIORITIES

Acknowledge women's contributions. Women have been working in cybersecurity for a century. Yet many of their stories have been sidelined because of the secrecy of the work, its wartime contexts or because male colleagues have been put in the limelight instead.

During the Second World War, the United States employed 10,000 women as 'code girls' to decipher encrypted messages sent by the Japanese and Germans. Likewise, the United Kingdom hired more than 7,000 women to work at Bletchley Park, its centre for cryptanalysis, where they made up about three-quarters of the workforce. And in 1942, actor and inventor Hedy Lamarr patented an encryption method for signalling to torpedoes that is now the basis of WiFi and bluetooth technology.

Elizebeth Smith Friedman helped to invent the science of cryptography for the US Federal Bureau of Investigation (FBI)[2]. Her techniques in the 1940s broke international spy rings, decoded three Nazi Enigma machines and contributed to the early work of the forerunner to the Central Intelligence Agency. Yet after the war, her elite code-breaking unit was shut down and various men took credit for her work, including her husband William Friedman and FBI director J. Edgar Hoover. Indeed, Hoover showed outright hostility towards women in this field — when he started as director of the FBI's predecessor in 1924, he fired all the female agents and banned further recruitment of women in these roles.

Women were the first programmers, calculating weapons trajectories by hand and entering them into the Electronic Numerical Integrator And Computer (ENIAC) at the University of Pennsylvania, Philadelphia, in the 1940s[3]. In fact, 'computer' originally referred not to the machine but to the women who programmed it. Other women developed the first programming languages, methods to detect intrusions into computer systems and network bridges between communication centres[4]. In the 1950s, African American female mathematicians at NASA calculated the aeronautical trajectories that put men on the Moon[5]. The proportion of women in computer science grew until the mid-1980s — the dawn of personal computing — when numbers dropped precipitously. Today, only around 18% of US computer-science majors are women, compared with around 37% in 1984.

"Women have held influential positions in US national cybersecurity."

Even so, in the past decade, women have held influential positions in US national cybersecurity. Theresa Payton was the first female chief information officer in the White House, under former president George W. Bush. Former president Barack Obama appointed Melissa Hathaway in 2009 as his first 'cyber czar', in the role of acting senior director for cyberspace for the National Security Council. Letitia Long was the first woman to head a major US intelligence agency, as director of the National Geospatial-Intelligence Agency from 2010 to 2014. This supplied the satellite, geographical and social-media data that enabled Osama bin Laden's capture. Janet Napolitano headed the Department of Homeland Security (DHS) from 2009 to 2013, and Kirstjen Nielsen has been at the helm since 2017. Jeannette Manfra, the chief cybersecurity official for the DHS, is leading the investigation into Russian hacking of US voter registration rolls before the 2016 presidential election.

Research leadership is crucial because it dictates the direction of security technologies and strategies. From 2009 to 2012, Regina Dugan was the first female director of the Defense Advanced Research Projects Agency (DARPA), the research wing of the military that helped to develop the Internet and the Global Positioning System. Her priorities included machine intelligence, flexible and manoeuvrable shape-shifting devices, and soldier telepathy using brain-wave mapping for communicating without speech. Dugan has since run technology programmes at Google and Facebook. From 2008 to 2012, Lisa Porter was founding director of 'DARPA for spies' — the Intelligence Advanced Research Projects Activity. She led investigations into quantum computing, biometric fingerprint identification and cloaking devices.

Although there is a predominance of white women in these positions, women of colour are making inroads. Quiessence Phillips, an African American, has been selected as deputy chief information security officer of cyber command for the City of New York. And Indian computer scientist Aanchal Gupta is director of security at Facebook.

Other women are taking more underground roles — as cyberspies[6]. Former judge Shannen Rossmiller gathered global online intelligence for the FBI after the terrorist attacks of 11 September 2001. By posing as male militants from Iraq and Afghanistan in extremist chat rooms, she exposed weapon caches, bomb plots and terror cells in more than 200 operations. Indeed, 35% of people who work in the intelligence field are female.

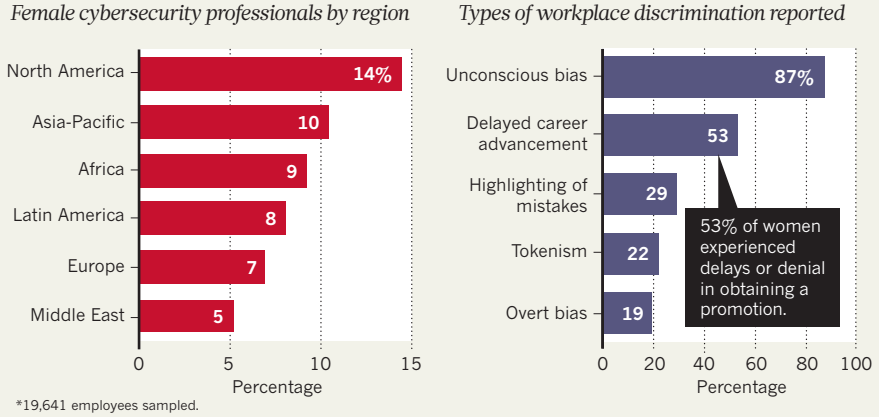
Meanwhile, cybersleuths like Kimberly Ritter are fighting crimes such as online sex trafficking. Ritter's work inspired computer scientists to develop an app called Traffickcam that enables the public to upload photographs of hotel rooms to a database. By matching these to images in advertisements for escorts, law enforcement agencies can improve the way they track down victims and their traffickers.

But breaking the glass ceiling is not enough. Institutional barriers also need to be overcome.

Recognize diverse expertise. Despite being few in number, female candidates for cybersecurity jobs tend to be more educated

WOMEN IN CYBERSECURITY

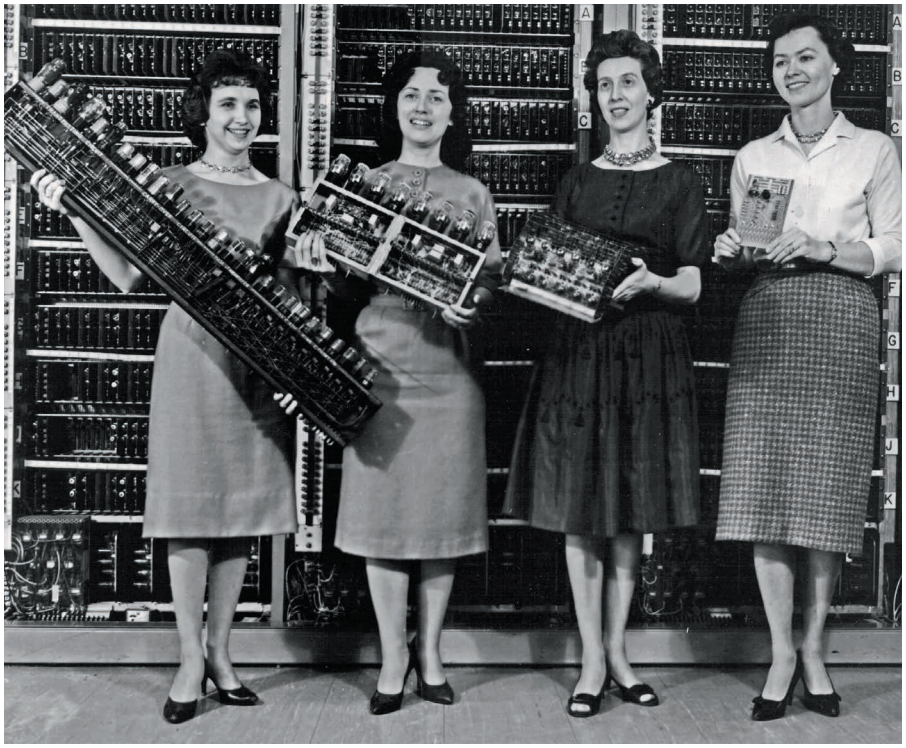
Hostile work cultures, stereotypes and discrimination are limiting the numbers* of female cybersecurity professionals (left). Just over half of women in cybersecurity say that they have experienced gender discrimination (right), compared with 15% of men.



*19,641 employees sampled.

SOURCE: 2017 GLOBAL INFORMATION SECURITY WORKFORCE STUDY

U.S. ARMY



Female programmers and mathematicians display parts of early computers at the US Army Ballistics Research Laboratory in 1962.

than their male counterparts. Women professionals are more likely to have a master's degree or higher (51% for women globally, compared with 45% of men). Women also tend to bring wider expertise. Although both female and male employees train extensively in computer science, information and engineering, women's degrees are more likely to come from fields such as business, mathematics and social science (44% for women, compared with 30% for men).

This is crucial because cybersecurity jobs demand diverse skills. Professionals must understand network security, risk mitigation and information protection, and be prepared for future activities in artificial intelligence, machine learning and virtual-reality mapping. They need to manage projects, navigate legal and compliance codes, and work in sectors from health care to law enforcement[4].

But training beyond fields in science, technology, engineering and maths (STEM) is not generally rewarded. Most cybersecurity employers view computer science or engineering backgrounds as a priority. Yet even some big tech companies are changing their outlook. In 2011, Microsoft co-founder Bill Gates disparaged liberal-arts education. Now, the company's president Brad Smith argues that such training is crucial for the future of computing, especially artificial intelligence. Google executives were shocked after they analysed their workforce data and found that STEM expertise was the least important factor associated with employees' success. Instead, qualities such as being a good coach, problem-solver or critical thinker ranked higher.

Shed sexist images. The two fields that are most closely associated with cybersecurity — IT and the military — are plagued by cultures that are hostile towards women.

The IT industry reveres the hacker persona — a loner, typically male and white, working all night and forgoing other spheres of life. Some employees might identify with this image. Nonetheless, employers often use it as a standard for hiring and promoting, even though the workforce has diversified. As ethnomathematician Ron Eglash observed in 2002, these racial and gender premises of the hacker stereotype are being challenged by emerging groups such as "Black geeks, Asian American hipsters, and geek grrrls"[7].

Sexist attitudes are rife in California's Silicon Valley, exemplified by the memo leaked in 2017 from a male employee of Google arguing that women are biologically ill-suited to the technology field. The ride-hailing firm Uber received more than 200 claims of sexual harassment, discrimination and inappropriate behaviours from employees, according to an investigation at its San Francisco headquarters in 2017. The US federal government has filed lawsuits against tech firms for gendered wage discrimination.

The soldier image is rooted in military legacies. Women in cybersecurity often report working with an 'old boys club' of former intelligence and military officers[8]. Job postings call for "ninjas" and "cyberwarriors". The language of cybersecurity reflects this ethos of defending networks against threats from intruders. By contrast, the concept of information security — centred on creating safe, effective systems and protecting humans who use them — describes the job better and is more widely appealing to diverse practitioners, including women.

Cybersecurity conferences are notoriously male-dominated in number and hypermasculine in behaviour. A female attendee can be the sole woman in a group of 100 men. Two of the largest cybersecurity conferences, DEF CON and Black Hat, are held in Las Vegas, Nevada — a city long associated with the objectification of women. Women at these meetings have described experiences to scholars and online peer networks of being groped and asked by male attendees if they are a secretary or a prostitute.

The impacts are clear. More than half of women in cybersecurity around the world (51%) say that they have experienced gender discrimination, compared with 15% of men. This is sometimes overt but more often subtle — through tokenism, unconscious bias, the highlighting of mistakes, or denials and delays in career advancement. Female cybersecurity employees report a pay gap of 3–6% compared with male employees. This is much smaller than the 28% wage gap in the computing industry, but such losses accumulate over the course of a career. In the past couple of years, the gap has widened for female managers.

Women in technology leave their jobs at a higher rate than their male colleagues. The costs for US firms of losing and rehiring professionals who quit because of gender, racial, sexuality or religious bias are around $64 billion annually.

Realize that women and girls are prime targets of cybercrime. Women in the United States were 26% more likely than men to experience identity theft in 2008, often involving the fraudulent use of a bank account or credit card. Two-thirds of victims lost money. On average, women also took longer than men to notice the breach: 83 versus 45 days. This is partly because men are more likely to bank and shop online, and so receive automatic notifications within hours — much faster than the weeks it can take to spot unauthorized transactions on monthly financial statements. Women in the United States also live in poverty to a greater degree than men do, and are less able to invest in online security services, freezing credit scores or hiring lawyers.

Some cybercrimes, such as 'sextortion', are directed at women and girls. Criminals trick their targets, using e-mails infected with software viruses, for instance, to gain access to their computers. Perpetrators can search for photos on hard drives or use webcams to

watch women and girls. They then blackmail targets by threatening to post images and videos on child pornography websites, to compel further sexual activity. The extortion can extend for years, because images can be permanently installed on multiple platforms. One perpetrator might have hundreds of targets. For example, 78 criminal cases of sextortion filed since 2016 may involve as many as 6,500 victims across 52 jurisdictions (US and international), 29 US states or territories and 3 foreign countries.

Strangers are usually assumed to be the culprits. In reality, women's spouses, boyfriends or family members often initiate security breaches. Abusers glean passwords through key-logging devices or by coercing their targets to hand over passwords. Misuse of technology online is linked to physical abuse offline. In a national survey, 97% of US domestic abuse shelters reported that their female clients had been harassed through technology.

NEXT STEPS

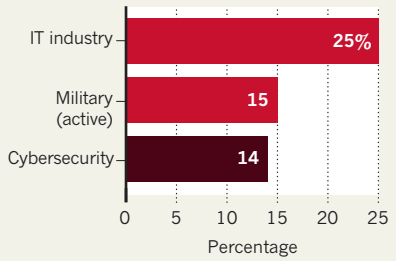
Cybersecurity needs to become more accepting of and welcoming to women. Schools and universities should emphasize the field's creativity and real-world applications. Programmes that promote technology for young women and girls should be encouraged, such as Girls Who Code, which aims to increase women in computer science and engineering. In another initiative, the US Girl Scouts organization is rolling out cybersecurity as one of its skill badges.

Media outlets and conference organizers should invite female experts and speakers. There are more than enough to choose from: the Grace Hopper Celebration (named after one of the first women coders) meets annually and brought together around 18,000 women technologists last year. WiCyS and the Diana Initiative are smaller but more specialized networks that also promote women in cybersecurity.

Employers should craft job advertisements that use inclusive wording, and seek candidates beyond computer science and the military, such as from the social sciences, humanities, law and public policy. Recruiters should use diverse selection panels

SISTER FIELDS

Related fields have relatively more women than does cybersecurity.



NASA mathematician Katherine Johnson did the calculations that put men on the Moon.

NASA/DONALDSON COLLECTION/GETTY

and gender-blinded screening of résumés. Women should be hired in cohorts to avoid isolation and experiences of tokenism.

Retaining women requires fair career trajectories. Employers should track and enforce gender parity in evaluations, promotions and salaries. Some firms are showing progress. The Anita Borg Institute's list of Top Companies for Women Technologists highlighted the firms Accenture, Geico and ThoughtWorks as its winning examples in 2017.

"Retaining women requires fair career trajectories."

Researchers need to answer pressing questions about gender in cybersecurity. For example, how can retail and credit firms better protect women from the fallout of hacks and identity theft? How can domestic partners be prevented from accessing passwords? Regional disparities also need examining. For instance, Europe has fewer women in cybersecurity (7%) than North America does (14%), despite similar levels of industrialization. India has a better record of graduating female computer programmers (30%) than does the United States (21%)[9].

Cybersecurity professionals and organizations need to build partnerships to understand the types of people who are affected by cybercrime. In the United States, organizations might include the National Network to End Domestic Violence, the National Association for the Advancement of Colored People, UnidosUS (a non-profit Latino advocacy organization), the Federal Trade Commission and the Consumer Financial Protection Agency.

The purpose and practice of cybersecurity must be questioned. Huge amounts of money, technology and resources are often allocated to command-and-control strategies that can be inefficient and counterproductive[10]. Common-sense solutions, such as enforcing implementation of security patches and strengthening privacy protections on consumer electronics, can be simpler, cheaper and more effective.

Security systems must protect everyone, equally. Celebrating, attracting, training and retaining a greater diversity of scholars and technicians in information-security research, business and governance are steps in that direction. ■

Winifred R. Poster *is a lecturer in international affairs at Washington University, St. Louis, Missouri, USA.*
e-mail: wposter@wustl.edu

1. Browne, S. *Dark Matters: On the Surveillance of Blackness* (Duke Univ. Press, 2015).
2. Fagone, J. *The Woman Who Smashed Codes* (HarperCollins, 2017).
3. Light, J. S. *Technol. Cult.* **40,** 455–483 (1999).
4. Shumba, R. *et al.* Cybersecurity, Women and Minorities. *Proc. ITiCSE-WGR* **June, July,** 1–14 (2013).
5. Shetterly, M. L. *Hidden Figures* (HarperCollins, 2016).
6. Poster, W. R. in *Globalization, Technology Diffusion and Gender Disparity: Social Impacts of ICTs* (eds Pande, R. & van der Weide, T. P. 247–260 (IGI Global, 2012).
7. Eglash, R. *Social Text* **20,** 49–64 (2002).
8. D'Hondt, K. *Women in Cybersecurity*. Master's thesis, Harvard Kennedy School (2016).
9. Poster, W. R. *Gend. Sex. Fem.* **1,** 37–52 (2013).
10. Molotch, H. *Against Security* (Princeton Univ. Press, 2014).

CORRECTIONS

In data used for the graph 'Open countries have impact' in the Comment 'Open countries have strong science' (*Nature* **550,** 32–33; 2017), some articles classified into more than one field were counted twice. The online version of the graph has been updated to show disaggregated counts. The categorization of countries has not changed.

In the Comment 'How to make replication the norm' (*Nature* **554,** 417–419; 2018) mistakenly stated that only authors of non-replicated articles from the 3ie project described antagonism. In fact, authors of both replicated and non-replicated studies did. Also, the number of replications was 21, not 20. The data set is now available as supplementary information.

The Comment 'Smartphones are bad for some teens, not all' (*Nature* **554,** 432–434; 2018) misrepresented the results from the study on depressive episodes. The initial year should have been 2005, not 2004. And the rise between 2005 and 2014 should have been in percentage points, not per cent.

SOURCES: NATL CENTER FOR WOMEN IN TECHNOLOGY/PEW RESEARCH CENTER/ISC2/FROST & SULLIVAN

CORRECTION

In the Comment 'Cybersecurity needs women' (*Nature* **555**, 577–580; 2018), the photo of female programmers was captioned incorrectly. They were at the US Army Ballistics Research Laboratory in 1962, not working on ENIAC at the University of Pennsylvania in the 1940s. Also, the figure of 57% cited for women in the US workforce was actually for women in the US professional workforce.