2016
HALIFAX
PAPERS

HALIFAX
INTERNATIONAL SECURITY FORUM

NOVEMBER 18-20, 2016

SPIES LOVE US: PROTECTING INFORMATION IN THE AGE OF OPENNESS

— Heather M. Roff

In 1985, Aldrich "Rick" Ames began his infamous career as a mole for the former Soviet Union's KGB. Ames, with already 20 years of service in the Central Intelligence Agency, flipped to the other side. He claimed that his primary motivation was money, and in an interview in the mid 1990s, shortly after being caught, he surmised that he was operative for so long because he kept things "small."

In other words, when there are big bureaucracies at play with lots of information, it is easy to slip under the radar if you keep your ambitions in check.

Today, we would do well to remind ourselves of Ames and the role that information has always played. Information is the most valued currency, and being able to manipulate beliefs about information is equally as powerful. This is where our present day struggle to protect information begins to feel somehow new or different.

The huge "hacks" that dump zettabytes of information into the hands of nefarious actors, the ease with which they seem to do it and the inability to do much about it, makes it feel as if we have collectively failed in keeping our most prized digital possessions secure.

There is some truth here, but I would not say that we have entered a completely new age and are struggling with never-before-seen problems. Rather, the newness is just that adversaries have never before had so many open targets. Rick Ames had to give up names of fellow spies, and he had to be paid for his risk, but, now, nefarious adversaries do not have to undertake risk, and they can pull all of this information from outside the territory in which they are residing.

The volume of information is now astounding. If Ames handed over the equivalent of a few bankers boxes worth of information, the OPM hack—assuming smallish personnel files—would amount to backing up 160 tractor trailers to the Pentagon and stacking them from floor to ceiling. That sort of operation just couldn't have happened before.

Why is it so easy for our security to be compromised now? I would say for a variety of reasons spanning the physical structures that allow data flow, like undersea cables, through the processes that permit and regulate data flows, such as internet protocols and the difficulties of writing secure software with no vulnerabilities, to the ever-present fact that humans can be duped, manipulated or short-sighted.

Adding all of these things together with the reality that we have 3.4 billion internet users today—with an estimated 1.4 billion additional users in the next ten years—connected to 24 billion devices worldwide, the potential attack space appears to present an insurmountable challenge.

However, we ought not to take the present and coming difficulties of data protection as evidence that nothing that is digital is secure. Going back to a pencil and paper is no guarantee of data security either—as Rick Ames proves. Rather, we must think through our digital realities and leverage technology to overcome our known vulnerabilities and weaknesses.

First, we must not demonize encryption, but rather invest in it, for this is what actually enables security for everyone. Second, we must explore artificial intelligence (AI) for network protection. We need machine learning to make sense of the

massive amounts of data so that it becomes useful for human cyber security experts to make the right decisions. AI agents will patrol our networks and look for abnormalities and irregularities that humans could never possibly see.

However, this security also requires that we ensure that the design of these AI agents and what they are doing is as transparent to us as possible. We ought not be afraid that using digital information is an invitation for exploitation. But, we need to think critically about how to design these systems for human users. If we fail to understand the information presented, in our algorithmically determined world, then we cannot know if it is biased, true or false. This is as dangerous for security experts as it is for the average citizen.

Ultimately, there is a level of risk acceptance in the digital domain. This risk acceptance, however, is not an acceptance that all information is insecure, but that perfect security is an illusion. The technologies we develop to enhance our information security, as well as the strategies for their use, must depend on a delicate balance of "technological realism" and social science. That is, rather than thinking there is an easy technological fix, or that technology saves, we ought to admit its limits. For these limits are uniquely and inherently intertwined with human behavior and beliefs. The human factor can never be overlooked or under estimated. This means that information "leakage" is always a possibility (and perhaps inevitable), as no one can anticipate the moles or the whistleblowers. Protecting information means being better aware of how we protect ourselves in this new age, and remembering that because we live amid huge data, big bureaucracies and big business, we are all comparatively "small."

Heather M. Roff is a Senior Research Fellow at the University of Oxford, a Research Scientist at Arizona State University, and a Fellow at New America.