December 9, 2013
Spies Infiltrate a Fantasy Realm of Online Games
By MARK MAZZETTI and JUSTIN ELLIOTT
Not limiting their activities to the earthly realm, American and British spies have infiltrated the fantasy worlds of World of Warcraft and Second Life, conducting surveillance and scooping up data in the online games played by millions of people across the globe, according to newly disclosed classified documents.

Fearing that terrorist or criminal networks could use the games to communicate secretly, move money or plot attacks, the documents show, intelligence operatives have entered terrain populated by digital avatars that include elves, gnomes and supermodels.

The spies have created make-believe characters to snoop and to try to recruit informers, while also collecting data and contents of communications between players, according to the documents, disclosed by the former National Security Agency contractor Edward J. Snowden. Because militants often rely on features common to video games — fake identities, voice and text chats, a way to conduct financial transactions — American and British intelligence agencies worried that they might be operating there, according to the papers.

Online games might seem innocuous, a top-secret 2008 N.S.A. document warned, but they had the potential to be a “target-rich communication network” allowing intelligence suspects “a way to hide in plain sight.” Virtual games “are an opportunity!” another 2008 N.S.A. document declared.

But for all their enthusiasm — so many C.I.A., F.B.I. and Pentagon spies were hunting around in Second Life, the document noted, that a “deconfliction” group was needed to avoid collisions — the intelligence agencies may have inflated the threat.

The documents, obtained by The Guardian and shared with The New York Times and ProPublica, do not cite any counterterrorism successes from the effort. Former American intelligence officials, current and former gaming company employees and outside experts said in interviews that they knew of little evidence that terrorist groups viewed the games as havens to communicate and plot operations.

Games “are built and operated by companies looking to make money, so the players’ identity and activity is tracked,” said Peter W. Singer of the Brookings Institution, an author of “Cybersecurity and Cyberwar: What Everyone Needs to Know.” “For terror groups looking to keep their communications secret, there are far more effective and easier ways to do so than putting on a troll avatar.”

The surveillance, which also included Microsoft’s Xbox Live, could raise privacy concerns. It is not clear exactly how the agencies got access to gamers’ data or communications, how many players may have been monitored or whether Americans’ communications or activities were captured.

One American company, the maker of World of Warcraft, said that neither the N.S.A. nor its British counterpart, the Government Communications Headquarters, had gotten permission to gather intelligence in its game. Many players are Americans, who can be targeted for surveillance only with approval from the nation's secret intelligence court. The spy agencies, though, face far fewer restrictions on collecting certain data or communications overseas.

"We are unaware of any surveillance taking place," said a spokesman for Blizzard Entertainment, based in Irvine, Calif., which makes World of Warcraft. "If it was, it would have been done without our knowledge or permission."

A spokeswoman for Microsoft declined to comment. Philip Rosedale, the founder of Second Life and a former chief executive officer of Linden Lab, the game's maker, declined to comment on the spying revelations. Current Linden executives did not respond to requests for comment.

A Government Communications Headquarters spokesman would neither confirm nor deny any involvement by that agency in gaming surveillance, but said that its work is conducted under "a strict legal and policy framework" with rigorous oversight. An N.S.A. spokeswoman declined to comment.

Intelligence and law enforcement officials became interested in games after some became enormously popular, drawing tens of millions of people worldwide, from preteens to retirees. The games rely on lifelike graphics, virtual currencies and the ability to speak to other players in real time. Some gamers merge the virtual and real worlds by spending long hours playing and making close online friends.

In World of Warcraft, players share the same fantasy universe — walking around and killing computer-controlled monsters or the avatars of other players, including elves, animals or creatures known as orcs. In Second Life, players create customized human avatars that can resemble themselves or take on other personas — supermodels and bodybuilders are popular — who can socialize, buy and sell virtual goods, and go places like beaches, cities, art galleries and strip clubs. In Microsoft's Xbox Live service, subscribers connect online in games that can involve activities like playing soccer or shooting at each other in space.

According to American officials and the documents, spy agencies grew worried that terrorist groups might take to the virtual worlds to establish safe communications channels.

In 2007, as the N.S.A. and other intelligence agencies were beginning to explore virtual games, N.S.A. officials met with the chief technology officer for the manufacturer of Second Life, the San Francisco-based Linden Lab. The executive, Cory Ondrejka, was a former Navy officer who had worked at the N.S.A. with a top-secret security clearance.

He visited the agency's headquarters at Fort Meade, Md., in May 2007 to speak to staff members over a brown bag lunch, according to an internal agency announcement. "Second Life has proven that virtual worlds of social networking are a reality: come hear Cory tell you why!" said the announcement. It

added that virtual worlds gave the government the opportunity “to understand the motivation, context and consequent behaviors of non-Americans through observation, without leaving U.S. soil.”

Mr. Ondrejka, now the director of mobile engineering at Facebook, said through a representative that the N.S.A. presentation was similar to others he gave in that period, and declined to comment further.

Even with spies already monitoring games, the N.S.A. thought it needed to step up the effort.

“The Sigint Enterprise needs to begin taking action now to plan for collection, processing, presentation and analysis of these communications,” said one April 2008 N.S.A. document, referring to “signals intelligence.” The document added, “With a few exceptions, N.S.A. can’t even recognize the traffic,” meaning that the agency could not distinguish gaming data from other Internet traffic.

By the end of 2008, according to one document, the British spy agency, known as GCHQ, had set up its “first operational deployment into Second Life” and had helped the police in London in cracking down on a crime ring that had moved into virtual worlds to sell stolen credit card information. The British spies running the effort, which was code-named Operation Galician, were aided by an informer using a digital avatar “who helpfully volunteered information on the target group’s latest activities.”

Though the games might appear to be unregulated digital bazaars, the companies running them reserve the right to police the communications of players and store the chat dialogues in servers that can be searched later. The transactions conducted with the virtual money common in the games, used in World of Warcraft to buy weapons and potions to slay monsters, are also monitored by the companies to prevent illicit financial dealings.

In the 2008 N.S.A. document, titled “Exploiting Terrorist Use of Games & Virtual Environments,” the agency said that “terrorist target selectors” — which could be a computer’s Internet Protocol address or an email account — “have been found associated with Xbox Live, Second Life, World of Warcraft” and other games. But that document does not present evidence that terrorists were participating in the games.

Still, the intelligence agencies found other benefits in infiltrating these online worlds. According to the minutes of a January 2009 meeting, GCHQ’s “network gaming exploitation team” had identified engineers, embassy drivers, scientists and other foreign intelligence operatives to be World of Warcraft players — potential targets for recruitment as agents.

At Menwith Hill, a Royal Air Force base in the Yorkshire countryside that the N.S.A. has long used as an outpost to intercept global communications, American and British intelligence operatives started an effort in 2008 to begin collecting data from World of Warcraft.

One N.S.A. document said that the World of Warcraft monitoring “continues to uncover potential Sigint value by identifying accounts, characters and guilds related to Islamic extremist groups, nuclear

proliferation and arms dealing." In other words, targets of interest appeared to be playing the fantasy game, though the document does not indicate that they were doing so for any nefarious purposes. A British document from later that year said that GCHQ had "successfully been able to get the discussions between different game players on Xbox Live."

By 2009, the collection was extensive. One document says that while GCHQ was testing its ability to spy on Second Life in real time, British intelligence officers vacuumed up three days' worth of Second Life chat, instant message and financial transaction data, totaling 176,677 lines of data, which included the content of the communications.

For their part, players have openly wondered whether the N.S.A. might be watching them.

In one World of Warcraft discussion thread, begun just days after the first Snowden revelations appeared in the news media in June, a human death knight with the user name "Crrassus" asked whether the N.S.A. might be reading game chat logs.

"If they ever read these forums," wrote a goblin priest with the user name "Diaya," "they would realize they were wasting" their time.

Even before the American government began spying in virtual worlds, the Pentagon had identified the potential intelligence value of video games. The Pentagon's Special Operations Command in 2006 and 2007 worked with several foreign companies — including an obscure digital media business based in Prague — to build games that could be downloaded to mobile phones, according to people involved in the effort. They said the games, which were not identified as creations of the Pentagon, were then used as vehicles for intelligence agencies to collect information about the users.

Eager to cash in on the government's growing interest in virtual worlds, several large private contractors have spent years pitching their services to American intelligence agencies. In one 66-page document from 2007, part of the cache released by Mr. Snowden, the contracting giant SAIC promoted its ability to support "intelligence collection in the game space," and warned that online games could be used by militant groups to recruit followers and could provide "terrorist organizations with a powerful platform to reach core target audiences."

It is unclear whether SAIC received a contract based on this proposal, but one former SAIC employee said that the company at one point had a lucrative contract with the C.I.A. for work that included monitoring the Internet for militant activity. An SAIC spokeswoman declined to comment.

In spring 2009, academics and defense contractors gathered at the Marriott at Washington Dulles International Airport to present proposals for a government study about how players' behavior in a game like World of Warcraft might be linked to their real-world identities. "We were told it was highly likely that persons of interest were using virtual spaces to communicate or coordinate," said Dmitri

Williams, a professor at the University of Southern California who received grant money as part of the program.

After the conference, both SAIC and Lockheed Martin won contracts worth several million dollars, administered by an office within the intelligence community that finances research projects.

It is not clear how useful such research might be. A group at the Palo Alto Research Center, for example, produced a government-funded study of World of Warcraft that found “younger players and male players preferring competitive, hack-and-slash activities, and older and female players preferring noncombat activities,” such as exploring the virtual world. A group from the nonprofit SRI International, meanwhile, found that players under age 18 often used all capital letters both in chat messages and in their avatar names.

Those involved in the project were told little by their government patrons. According to Nick Yee, a Palo Alto researcher who worked on the effort, “We were specifically asked not to speculate on the government’s motivations and goals.”

Justin Elliott is a reporter for ProPublica. Andrew W. Lehren contributed reporting.