



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

(S//SI) **Topic: Exploiting Terrorist Use of Games & Virtual Environments**

(TS//SI) **Issue:** We know that terrorists use many feature-rich Internet communications media for operational purposes such as email, VoIP, chat, proxies, and web forums and it is highly likely they will be making wide use of the many communications features offered by Games and Virtual Environments (GVE) by 2010. The SIGINT Enterprise needs to begin taking action now to plan for collection, processing, presentation, and analysis of these communications. With a few exceptions, NSA can't even recognize the traffic, and therefore it is impossible to even say what percentage of the environment is GVE; let alone determine how targets are using the communications features of GVEs. However, GVEs offer a SIGINT/HUMINT opportunity space and more research is needed to figure out effective exploitation.

(S//SI) GVEs today allow individuals to gather with like-minded others online. Many GVEs offer communications such as private chat (P2P), group chat, chat to an alias, and broadcast chat—both text and voice. Also many GVEs allow convergent technologies to intermingle such as XboxLive! which can be run via an Xbox360 gaming console and/or connect via a PC to normal MSN chat. Second Life offers the ability to anonymously text to a GSM phone (SMS) and soon they will offer anonymous voice calls so that phone numbers do not have to be known by either party and won't show up in collection. Some GVEs allow third party interfaces which allow limited functionality from a web browser. This overcomes obstacles such as a high-bandwidth requirement and or not being allowed to download software (think Internet café usage). In addition, many GVEs are able to be used via mobile devices connected wirelessly (phones, handhelds, laptops). Connected to the GVEs, specialized forums and other social networking sites have sprung up to provide an additional place to interact, connect, or share. These sites and any others can be advertised in the GVEs, so that if a terrorist web forum has to move locations it can be found by its members again. Areas/groups can be access-restricted, member-only. They are essentially private meeting places, and can be used for planning, comms, and training, etc. GVEs are used for collaboration; Forterra's 3D world is coming to JWICS to do this IC-wide.

(U//FOUO) GVEs have been made that reinforce prejudices and cultural stereotypes while imparting a targeted message or lesson both from the Western point of view and in the Middle East. America's Army is a U.S. Army produced game that is free download from its recruitment page and is acknowledged to be so good at this the army no longer needs to use it for recruitment, they use it for training. The Lebanese Hizballah has taken this concept and the same basic game design and made its own version of the game called Special Forces 2 (SF2), which its press section acknowledges is used for recruitment and training in order to prepare their youth to "fight the enemy", a radicalizing medium; the ultimate goal is to become a suicide martyr. One cannot discount the "fun factor" involved—it is important to hold your target audience's attention-- and makes ingesting the message not even noticeable. SF2 features multi-player, on-line text and voice chat for up to 60 players simultaneously, effectively acting like a VPN or private chat forum. SF2 is offered at \$10 a copy and so also goes to fund terrorist operations.

(S//SI) These games offer realistic weapons training (what weapon to use against what target, what ranges can be achieved, even aiming and firing), military operations and tactics, photorealistic land navigation and terrain familiarization, and leadership skills. While complete military training is best achieved in person, perfection is not always required to accomplish the mission. Some of the 9-11 pilots had never flown a real plane, they had only trained using

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Microsoft's Flight Simulator. When the mission is expensive, risky, or dangerous, it is often a wiser idea to exercise virtually, rather than really blow an operative up assembling a bomb or exposing a sleeper agent to law enforcement scrutiny. Militaries around the world use virtual simulators with great success and the Hizballah has even hooked up a Playstation controller to a laptop in order to guide some of its real missiles. Kuma Wars is a U.S. owned company that offers realistic battle simulation of real battles in Iraq usually one month after they actually happened. The player can re-do maneuvers in a lessons learned way for training, or you can switch sides and see how it works from the opposite side. It also provides real terrain features, such as real road signs from real roads in Iraq, and a simulated night-vision goggles environment.

(TS//SI) Al Qaida terrorist target selectors and GVE executables have been found associated with XboxLive, Second Life, World of Warcraft, and other GVEs in PINWALE network traffic, TAO databases, and in forensic data. Other targets include Chinese hackers, an Iranian nuclear scientist, Hizballah, and Hamas members. GCHQ has a vigorous effort to exploit GVEs and has produced exploitation modules in XboxLive! and World of Warcraft. After beta testing, they expect reporting to begin in April 2008. The FBI, CIA and the Defense Humint Service all have HUMINT operations in Second Life and other GVEs and are very interested in forming a deconfliction and tipping group that would be able to collaborate on operations.

(TS//SI) GVEs are an opportunity! We can use games for: CNE exploits, social network analysis, HUMINT targeting, ID tracking (photos, doc IDs), shaping activities, geo-location of target, and collection of comms. It has been well documented that terrorists are OPSEC and tech saavy and are only getting more so over time. These applications and their servers however, are trusted by their users and makes an connection to another computer on the Internet, which can then be exploited. Through target buddylists and interaction found in the gaming and on gaming web sites, social networks can be diagramed and previously unknown SIGINT leads and connections and terrorists cells discovered. GVEs can contain on-line presence indicators, geolocation, and ID tracking can be gleaned and used in apprehension operations.

(TS//SI) **Recommendation:** The amount of GVEs in the world is growing but the specific ones that CT needs to be methodically discovered and validated. Only then can we find evidence that GVEs are being used for operational uses. Protocol Exploitation, SFL, and TAO should begin profiling their databases and the GVEs for collection and exploitation possibilities. Open source (APSTARS) produced GVE lists and selectors should be used to run against UTT and other databases to check for cross matches to develop target selectors. CT SIGDEV along with CT TOPIs will study the collected traffic to find and track targets of interest. There should be a concentrated effort to conduct research into target use of GVEs, and signatures for survey collection should be developed. Targets and specific apps should be chosen to exploit to ensure that terrorists' GVE/social site usage is covered by SIGINT and the system is not left behind the times. All avenues should be taken to develop PES and CNE exploits as GVEs are found on target computers. We need to develop a viewer/db that allows linguist/analysts to view/experience voice/text/video traffic together and archive the GVE data associated with reporting. which will also be essential for Yahoo, Skype, webcam, VTCs and Biometrics.

(S//SI) CT SIGDEV/SSG should establish a process to deconflict IC-wide ops in GVEs and to develop strategy for collaboration. Members from at least CIA, FBI, DIA, NSA and GCHQ should participate to make the coordination significant. Members should have ability to check tasking, traffic, and status of current operations.