Homeland Security

Cyber - Control Security Mapping

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Homeland Security

Cyber - Control Security Mapping

Overview

Regulating the Internet into Tiers and Zones

Simenona Martinez

Cyber - Control Security Mapping: traces and tracks the digital footprints of every user's registered device with the assistance telecommunications towers and cyber - monitoring.

This would eliminate the anonymity in cyberstalking and sex trafficking crimes. This is also effective in prohibiting hacking and scams. This will prevent young girls from being blackmailed by predators by restricting criminals from access all together but also, those who are likely to offend according to their digital footprints. This would notify the authorities if a cell phone was used within a radius of prohibited persons.

IP addresses can be concealed by criminals hiding their VPNS or using a burner phone, however, burner phones are to require the same registration for all phones in use going forward. The method of cyber - cloaking will be reutilized for concealing data from user to user to further prevent hacking, as most notably used in cryptography.

The operation should be run on a federal and state level. Each state should have a task force.

Mapping out the internet just as the constellations, air, and the ocean RADAR, is critical. Every single device connected to the web must be registered by the at an subsidiary contacted to the Department of Homeland Security. The use of cell towers will be instrumental in determining locations. It is important to regulate the internet traffic from outside of the United States, particularly in high terrorism zones.

The ability to trace and track digital footprints is essential for cybersecurity and ultimately cyber safety. The ultimate goal is preventing cyber - crimes, and cyber - threats.

The CCSM Tiers

Tier 1: Restricted Access for children under 18.

Restricted google results based on age. Age-appropriate content and registered user interaction. Admin will record / log each user's incoming and outgoing content, sending out daily reports to parents.

Tier 2: General Access.

Tier 3: Risk Users.

These are the individuals who have committed crimes. Admin will record / log each user incoming and outgoing content, sending out daily reports to State Officials.

This tool would be helpful in counter - terrorism by restricting the flow of incoming intelligences from other territories with high terrorism rates, as well outgoing information which may compromise our citizens and therefore, our Nation.

Law enforcement agencies will be alerted if a Tier 3 user attempts to access information in the red zone.

The CCSM Zones

Red Zone:

Firearms, Child Pornography, Suicide / homicide methods, and various illegal activities.

Blue Zone:

Integrating social media networks; users will be reported to the state for cyberbullying, exploitation, harassment, or blackmailing. The users are heavily monitored, tracking their digital footprints to the federal communications department.

Yellow Zone:

Non - Citizen Restricted Access for users who are outside of the United States who have registered with the federal government to access us internet.

Artificial Intelligence would play a huge role in this process; however, it also requires oversight.

Anonemis Research
Simenona Martinez
AnonemisResearch.com