

Isaiah Browne
CYSE 201S
11/6/2024

Journal Entry 10

To understand and control the changes that technology causes in people's behavior, social relationships, and political results, a new area of national security called "social cybersecurity" has been created. As the digital world becomes easier to control, this means building the systems needed to protect society's most important ideals and functions. Instead of just protecting computer systems from cyberattacks like traditional cybersecurity does, social cybersecurity also tries to protect society from digital threats that use technology to attack people's behavior, social harmony, and trust.

People in both governments and non-government organizations can quickly change public opinion, social views, and political landscapes through cyberspace in modern warfare. Now there is a new kind of war: internet warfare. It is now common knowledge that information can be used as a weapon to weaken countries and make people less trusting of their government. A official declaration of war isn't needed for this kind of warfare; it happens all the time, and most of the time, no one can see it. It shapes the battlefield long before any fighting starts.

With social cybersecurity, which is sometimes called "cognitive hacking," technology is used to control and "hack" people by going after the beliefs and social structures that hold them together. For strategic effects on a world level, it uses mass communication, psychological tactics, and social science insights. The field of behavior science uses tools from many fields, like computer science, psychology, marketing, and even politics and society, to look at and guess patterns of behavior, from small actions by individuals to big trends in society as a whole.

More and more people think that social protection is important for keeping societies safe and stable in a time when information warfare can be just as important for national security as traditional military power.