# FORENSIC PSYCHOLOGY OF AUTONOMOUS SYSTEMS

Cyber-psychology is an emerging discipline that focuses on the study of human-machine interaction. Cyber-psychology studies how humans are impacted by technology, how they interact over online mediums, and the effect of cyberspace interactions on the minds of individuals.

# THE SIGNIFICANCE OF CYBER PSYCHOLOGY

As technology advances and increasingly continues to affect our modes of thinking, psychologists have decided to focus their efforts in a new field. The result is cyberpsychology, which has become a meeting point for psychologists and scientists representing a vast array of disciplinary concentrations.

Cyberpsychology.org, a resource by and for academics who negotiate the ongoing junctures of technology and psychology, provides a clear definition for cyberpsychology. It says, "the psychological phenomena which emerge as a result of the human interaction with digital technology, PARTICULARLY THE INTERNET." The interdisciplinary approach has received significantly more attention in scholarly circles because of its exploration of topics like:

- Online dating and relationships.
- Self-perception in an online space.
- Social media and cyberspace addiction.
- Regressive and problematic behavior types online.

Moreover, the scholars attached to this group find the blossoming field necessary because our world continues to blend technology and psychology.

# FORENSIC PSYCHOLOGY

While taking up forensic psychology the individual is trained to understand whether a person has committed an action usually a grave

one against another human being, by his or her own free will or due to mental disorder that inhibits.

Autonomous Systems provides comprehensive reviews of significant theoretical and applied developments that impact the engineering of autonomous and semiautonomous systems. The broad fields of control and robotics are the major areas covered, together with connections to theoretical and applied mechanics, optimization, communication, information theory, machine learning, computing, and signal processing.

# **RESPONSIBLE AI**

Responsible AI is a framework for bringing many of these critical. practices together. It focuses on ensuring the ethical, transparent and accountable use of AI technologies in a manner consistent with user expectations, organizational values and societal laws and norms.

If artificial or alien intelligences show evidence of being sentient, this philosophy holds that they should be shown compassion and granted rights. Joanna Bryson has argued that creating AI that requires rights is both avoidable, and would in itself be unethical, both as a burden to the AI agents and to human society.

Explainable AI and the pursuit of using technology and statistical methods to explain Machine Learning models, quickly became a much larger question. Best practices in applying AI is not just a statistical question, but a people and process question as well, which forms the key elements of Responsible AI. In order to achieve maximum transparency and understanding of AI, it is imperative to address and understand the full view of models and their impact. There are six categories that comprise the most critical themes in Responsible AI: Explainable AI, Interpretable Machine Learning technology, Ethical AI, Secure AI, Human-Centered AI, and Compliance.

Al deployers should consider our core themes of Responsible Al:

# EXPLAINABLE AI (XAI)

The ability to explain a model after it has been developed

#### INTERPRETABLE MACHINE LEARNING

Transparent model architectures and increasing how intuitive and understandable ML models can be

# ETHICAL AI

Sociological fairness in machine learning predictions (i.e., whether one category of person is being weighted unequally)

# SECURE AI

Debugging and deploying ML models with similar counter-measures against insider and cyber threats as would be seen in traditional software

# HUMAN CENTERED AI

User interactions with AI and ML systems

#### COMPLIANCE

Making sure your AI systems meet the relevant regulatory requirements whether that's with GDPR, CCPA, FCRA, ECOA or other regulations