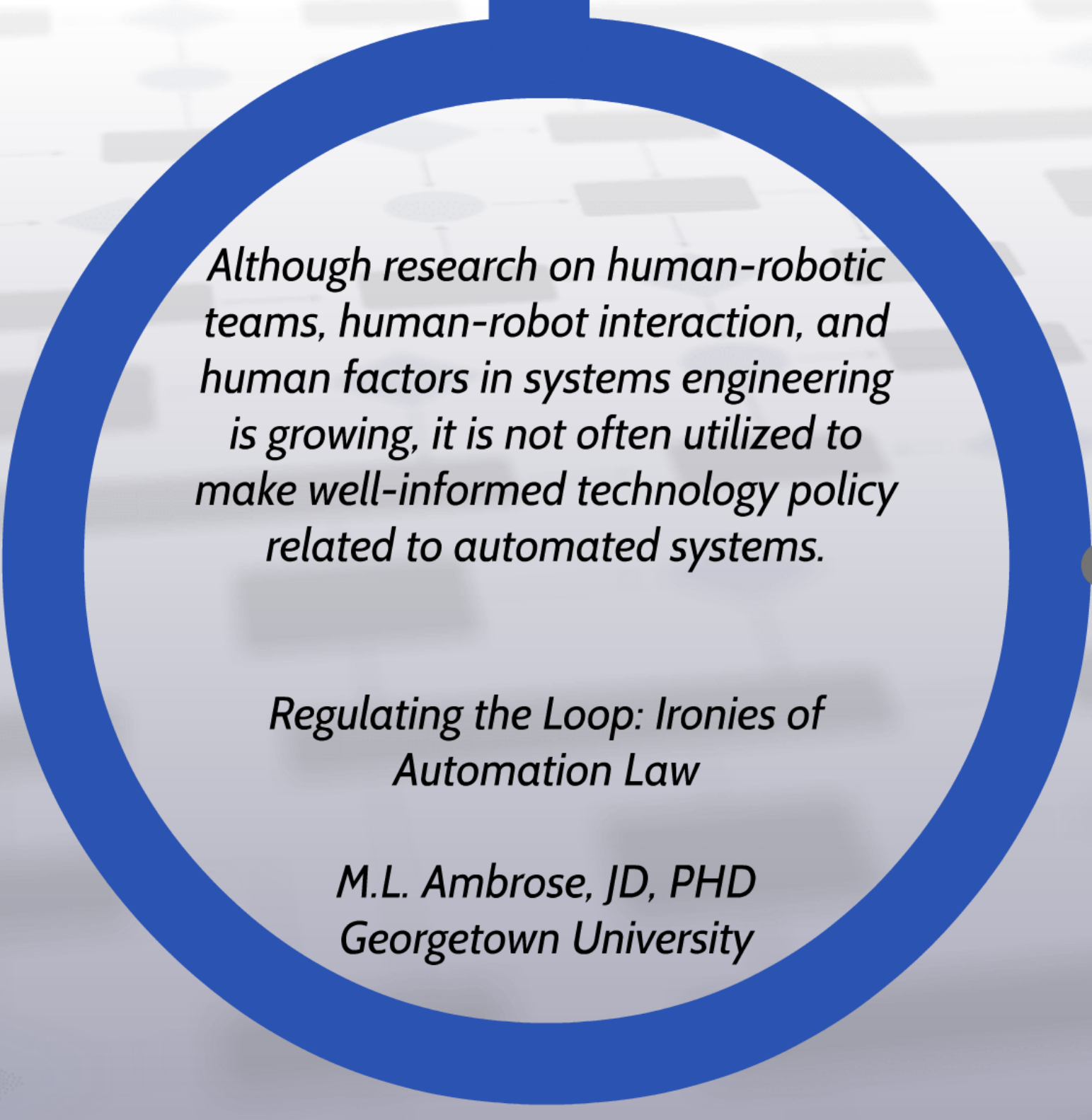


## Robot, Digital Forensics e Cyber Security

Giuseppe Vaciago

twitter: <https://twitter.com/giuseppevaciago>

linkedin: <https://www.linkedin.com/in/vaciago>



*Although research on human-robotic teams, human-robot interaction, and human factors in systems engineering is growing, it is not often utilized to make well-informed technology policy related to automated systems.*

*Regulating the Loop: Ironies of  
Automation Law*

*M.L. Ambrose, JD, PHD  
Georgetown University*

# Tre fattori

1. Tecnologia e connettività accessibili
2. Hardware versatile a basso costo
3. Infinite opportunità

\* *Federico Maggi, Giornata europea della privacy: "Il pianeta connesso. La nuova dimensione della privacy" 28 gennaio 2015.*

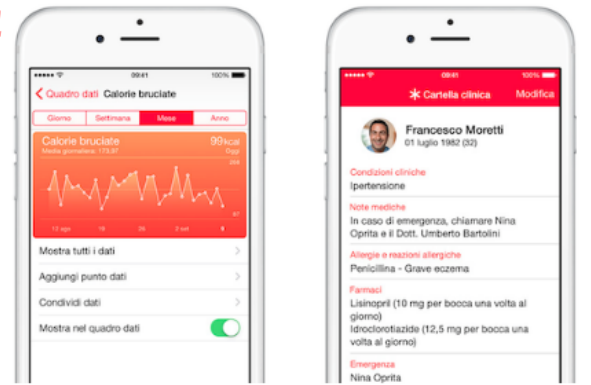
1930



2005



2014

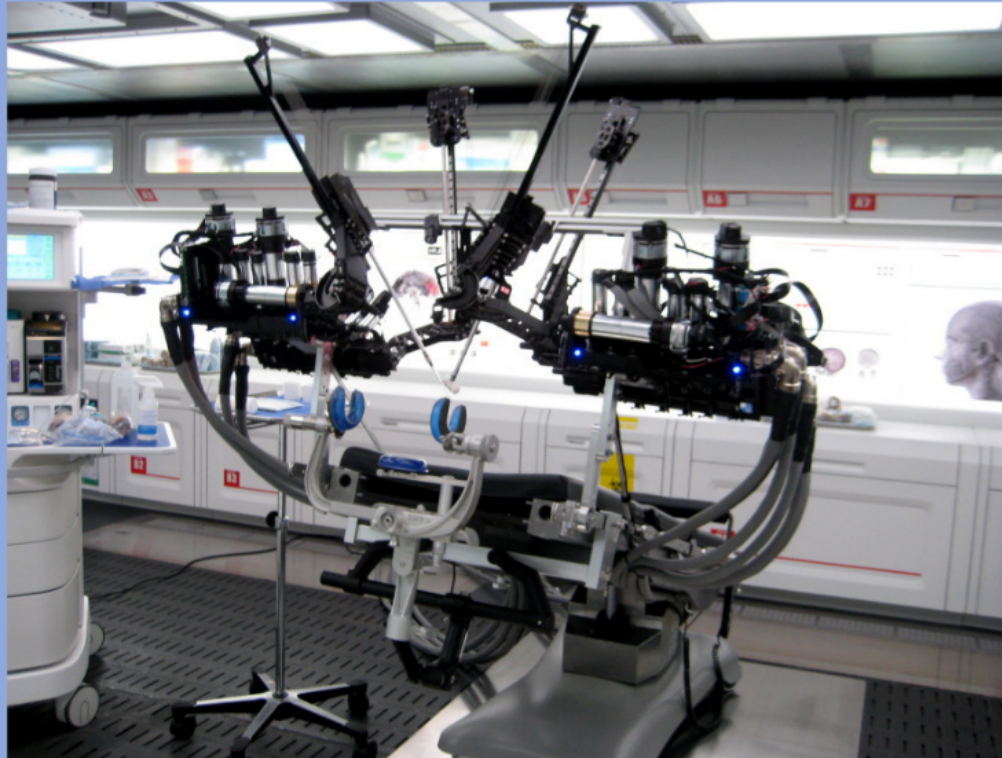




## *Infinite opportunità ...*



## Infiniti rischi ...



*To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots - 16 aprile 2015 - <http://arxiv.org/abs/1504.04339?con=&dom=pscaw&src=syndication>*

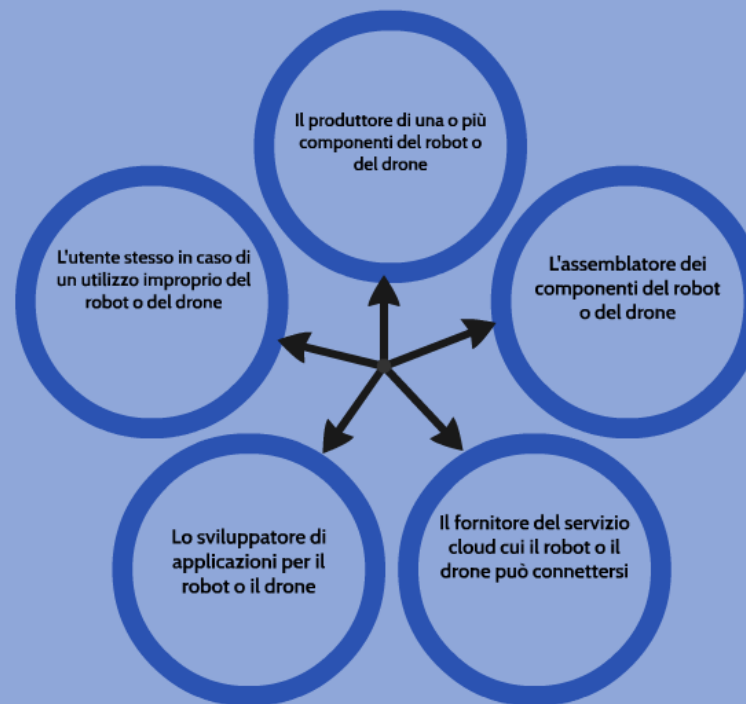
## *Digital (Robo) Forensics*

La digital forensics, ossia quel complesso di regole che consentono di recuperare, autenticare e studiare dati digitali, con particolare riferimento all'esame dei dati cancellati

In caso di malfunzionamento di un robot, dovrà essere verificato se tale malfunzionamento del robot sia stato generato dalle successive "implementazioni" hardware o software o a seguito di un "bug" di progettazione.



## *Allocazione delle responsabilità*



"Dovremmo considerare di creare un'esenzione di responsabilità per i produttori di robot rispetto all'uso che l'utente ne può fare attraverso le varie applicazioni che può installare. Una sorta di section 230 del Communication Decency Act"

Ryan Calo, Robotics and the New Cyberlaw, <http://www.roboticsbusinessreview.com/pdfs/roboticscyberlaw.pdf>



# *Quali sono le possibili soluzioni per garantire una maggiore security?*



- Allocazione di budget consistenti
- Security by Design e by Default
- Framework normativo - soft law o legge ad hoc?

# *Quali sono le possibili soluzioni per garantire una maggiore compliance in tema di digital forensics*

1. Attenta policy in tema di data retention
2. Procedure di Incident Response che prevedano l'applicazione delle best practices di digital forensics



=  
79054025  
255fb1a2  
6e4bc422  
aef54eb4



## *Un "classicone": il bilanciamento di interessi*

Tanto si eleva il livello di compliance in tema security e digital forensics quanto più si rischia di diminuire la garanzia che i nostri dati non vengano analizzati da terzi (confidenzialità).

- Maggiore retention del dato (IP e Log File)
- Maggiore controllo sui comportamenti degli utenti

Petanto, il rispetto della privacy dell'utente dovrà essere costantemente bilanciato con le esigenze di conservazione e di sicurezza del dato, proprie della digital forensics e della cyber security.

# *Conclusioni*

The human-automation relationship is not simple. “There will always be a human in the loop”

**BUT**

"The loop is an ill-defined parameter and in certain capacities, the human may not benefit, but harm, system performance".

M.L. Ambrose, JD, PHD, Regulating the Loop: Ironies of Automation Law, Georgetown University