Challenges of Encountering ISIS Network Recruitment: Algeria's Policies of Control and Censorship in the Digital Era

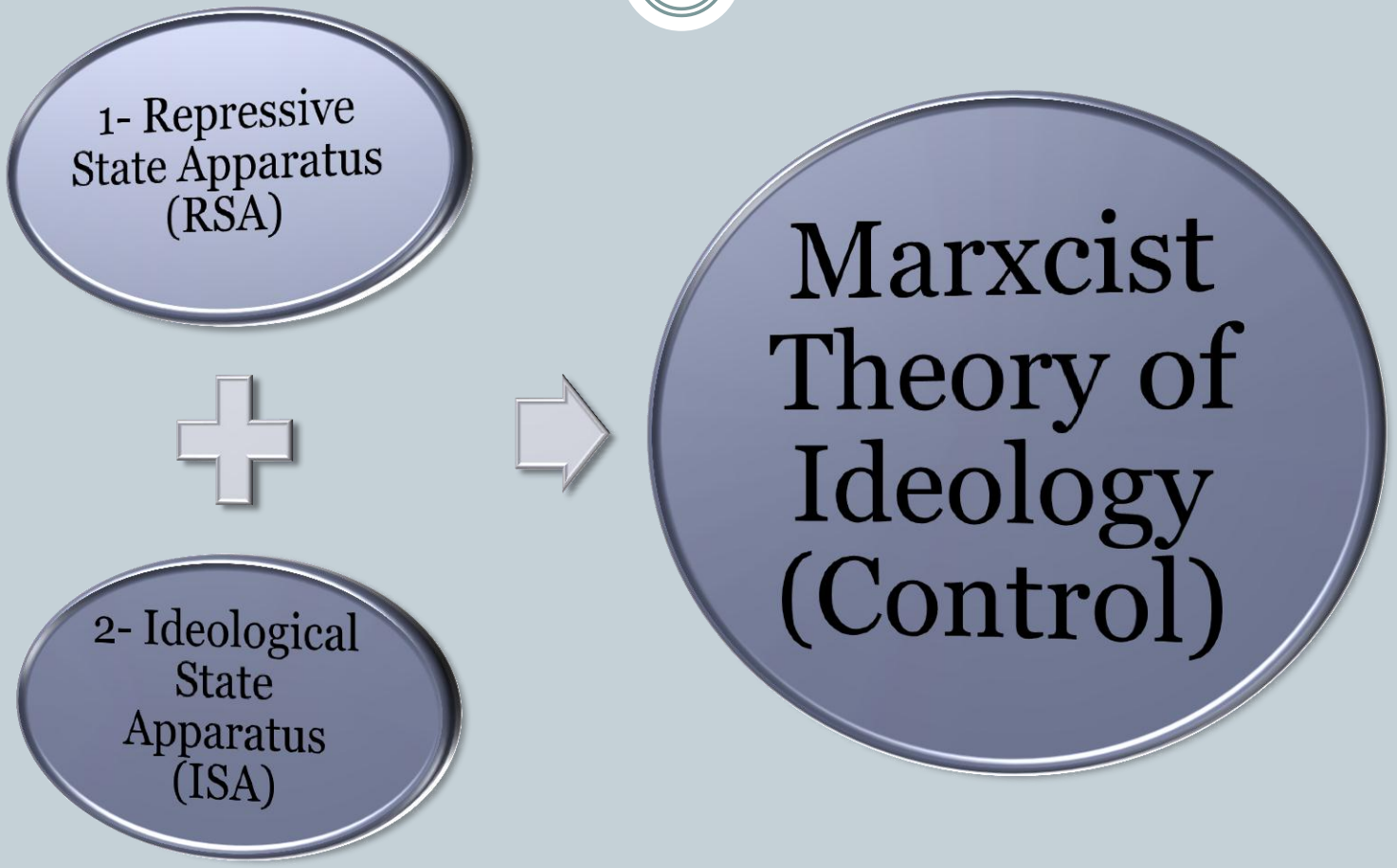
By: Mr. Mourad Aty
University of Guelma


CROSS
CRIME
SCENE

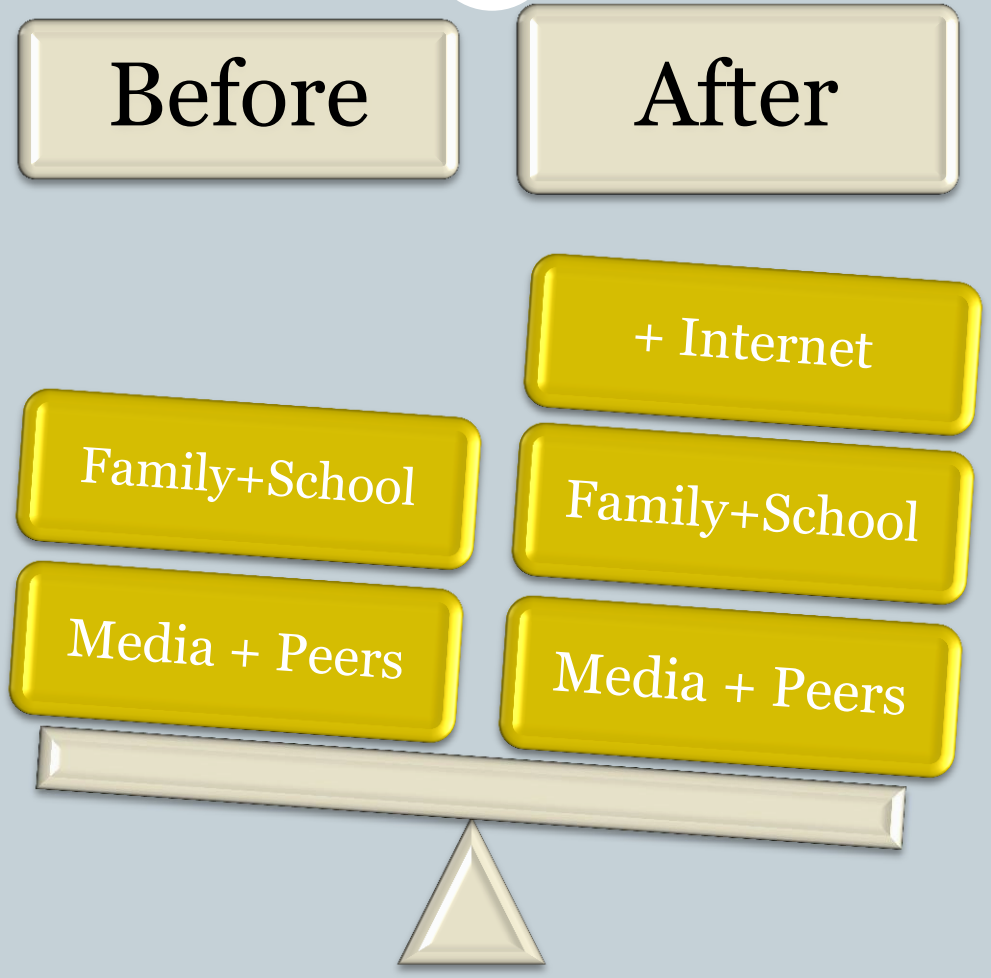
Criminals committing cybercrime use a number of methods, depending on their skill-set and their goal. Here are some of the different ways cybercrime can take shape:

- Theft of personal data
- Copyright infringement
- Fraud
- Sexploitation
- Cyberstalking
- Bullying

Marxcist Theory of Ideology



Process of Socializition



SEMINAR IN ALGIERS EXAMINES THE ROLE OF THE PROSECUTION IN TERRORIST CASES

The third in a series of seminars organized by the Counter-Terrorism Committee Executive Directorate (CTED) and tailored for prosecutors with experience in handling terrorist cases took place in Algiers from 5 to 7 June 2012. Close to 40 prosecutors and judges from different regions came together with representatives of international, regional and sub-regional organizations to examine their role in bringing terrorists to justice.

Keynote speakers included Mr. Kamal Razzak Bara, the Algerian President's Advisor for Counter-Terrorism; Mr. Francisco Madeira, Director of the African Centre for the Study and Research on Terrorism; and Mr. Mike Smith, Executive Director of CTED.

"Despite facing numerous challenges, prosecutors have been instrumental in preventing and combating

Global Counterterrorism Forum Co-Chairs' Fact Sheet: About the GCTF

Media Note

Office of the Spokesperson
Washington, DC
September 27, 2015

Below is the text of the Fact Sheet issued by the Co-Chairs (Turkey and the United States) of the Global Counterterrorism Forum on September 27, 2015.

Begin text:

The GCTF is an informal, multilateral counterterrorism (CT) platform focusing on identifying critical civilian CT needs, mobilizing the necessary expertise and resources to address such needs, and enhancing global cooperation. Launched at a ministerial meeting in New York on 22 September 2011, the Forum, with its 30 members (29 countries and the European Union), regularly convenes key CT policymakers and practitioners from nations around the world, as well as experts from the United Nations and other multilateral bodies. It has strengthened the

LES BLOGS D'EL WATAN

Algérie Montréal

Bandes originales

Outils Déontologique pour Journalistes Algériens

INSCRIPTION - CONNEXION

L'accès à l'article '**Naissance du gendarme du Net** : les vraies questions occultées' est restreint.
Merci de vous inscrire ou de vous connecter

Art. 20. — L'organe est habilité à requérir de tout organisme, institution ou service, tout document ou information nécessaire pour l'accomplissement des missions qui lui sont dévolues.

Art. 21. — Pour la prévention des infractions qualifiées d'actes terroristes ou subversifs et d'atteinte à la sûreté de l'Etat, l'organe est chargé à titre exclusif de la surveillance des communications électroniques, de la collecte et de l'enregistrement, en temps réel, de leur contenu ainsi que des perquisitions et des saisies dans un système informatique, sous l'autorité du magistrat compétent, et conformément aux dispositions de l'article 4 de la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009, susvisée.

Art. 22. — Pour l'exécution d'une opération de surveillance des communications électroniques, l'organe peut mettre en place une ou plusieurs unités de surveillance, dotées des moyens et équipements techniques nécessaires.

L'unité est composée de personnels techniques, agissant sous la direction et le contrôle d'un magistrat, secondé par un ou plusieurs officiers de police judiciaire relevant de l'organe.

Dans son action, l'unité se conforme aux dispositions de la législation en vigueur et des termes de l'autorisation délivrée par l'autorité judiciaire.

Ses travaux font l'objet d'un procès-verbal, établi conformément aux dispositions du code de procédure pénale.

Art. 23. — Ne peuvent participer à une opération de surveillance de communications électroniques que les membres de l'unité ou des unités auxquelles cette mission a été assignée par l'autorité judiciaire.

Pendant le déroulement de l'opération, toutes les mesures utiles sont prises par le chef de l'unité, en liaison avec les responsables concernés de l'organe, pour assurer la confidentialité de l'opération et la protection des informations recueillies de la surveillance.

Art. 24. — Pendant leur détention par l'organe, les informations recueillies lors des opérations de surveillance sont conservées suivant les règles applicables à la protection des informations classifiées.

Art. 25. — Les communications électroniques qui, font l'objet de surveillance sont enregistrées et transcrites suivant les conditions et formes prévues par le code de procédure pénale.

Les enregistrements et les transcriptions sont remis aux autorités judiciaires et aux services de police judiciaire compétents. Ces données sont conservées par les autorités judiciaires exclusivement, pendant la durée légale prévue par le législation en vigueur.

Art. 26. — Sous peine des sanctions pénales prévues par la législation en vigueur, les renseignements et données reçus ou recueillis par l'organe ne doivent pas être utilisés à des fins autres que la prévention et la lutte contre les infractions liées aux technologies de l'information et de la communication, conformément aux dispositions de la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009, susvisée.

Art. 27. — Les personnels de l'organe sont astreints au secret professionnel et à l'obligation de réserve.

Ceux d'entre eux qui sont appelés à accéder à des informations confidentielles sont soumis à une procédure d'habilitation.

Art. 28. — Les personnels de l'organe appelés à accéder à des informations confidentielles prêtent serment devant la Cour, avant leur installation, dans les termes suivants :

"أقسم بالله العلي العظيم أن أقوم بعملي أحسن قيام، وأن أخلص في تأدية مهمتي، وأن أكتم الأسرار والمعلومات أيا كانت التي اطلع عليها أثناء قيامي بعملي أو بمناسبته، وأن أسلك في كل الظروف سلوكا شريفا"

Art. 29. — Les personnels de l'organe sont placés sous l'autorité du directeur général.

Art. 30. — Les magistrats et les officiers de police judiciaire relevant de l'organe peuvent, dans ou à l'occasion de l'exercice de leurs fonctions, perquisitionner, conformément aux conditions et modalités prévues par la législation en vigueur et notamment le code de procédure pénale, tout lieu, structure ou organisme dont ils ont connaissance qu'ils détiennent et/ou utilisent des moyens et équipements destinés à la surveillance des communications électroniques.

En cas de constatation de faits susceptibles de qualification pénale, l'organe saisit le procureur général compétent pour d'éventuelles poursuites.

Art. 31. — L'organe peut demander l'assistance des fonctionnaires compétents aux ministères concernés dans le domaine des technologies d'information et de communication, conformément aux conditions et modalités fixées par la réglementation en vigueur.

Cyber Crime

We are building our lives around our wired and wireless networks. The question is, are we

In the News

10.27.15 **Headquarters**: NCSAM Cyber Tip: Social meda and the use of personal information....

10.21.15 **Washington, D.C.**: Director briefs House committee on threats, homeland security challenges....

10.20.15 **Headquarters**: NCSAM Cyber Tip: Defense in Depth for the everyday user.

10.20.15 **Knoxville**: Man gets 18 years for posing as a teenager to entice children online....

10.16.15 **Richmond**: Winchester Man Pleads Guilty to Computer Crime

More News

Cyber Fact Sheet

We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

The FBI certainly is. We lead the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. To stay in front of current and emerging trends, we gather and share information and intelligence with public and private sector partners worldwide.

In Depth

Key Priorities
- Computer and Network Intrusions
- Identity Theft
- Fraud: Internet Crime Complaint Center

Initiatives & Partnerships
- National Cyber Investigative Joint Task Force
- Cyber Task Forces
- iGuardian
- InfraGard: Protecting Infrastructure
- National Cyber-Forensics & Training Alliance
- Cyber Action Team

Cases & Takedowns
- Operation Ghost Click
- Coreflood Botnet
- 2,100 ATMs Hit at Once
- Operation Phish Fry
- Dark Market
- More

Wanted by the FBI
- Cyber's Most Wanted

Cyber Threats & Scams
- Internet Crime Reports
- National Cyber Awareness System
- Threat Overview: Testimony
- E-Scams & Warnings
- Common Internet Frauds
- Peer-to-Peer Networks
- Ransomware

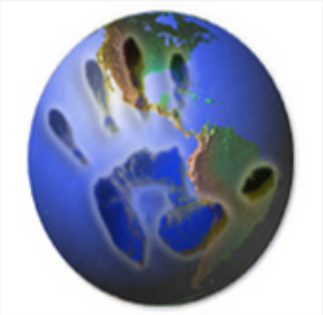
Protections
- Report a Cyber Incident
- Law Enforcement Cyber Incident Reporting (PDF)
- Get Educated on Internet Fraud
- How to Protect Your Computer
- Parent's Guide to Internet Safety

More Resources
- DOJ Computer Crime & Intellectual Property Section
- National Strategy to Secure Cyberspace
- Secret Service Electronic Crimes Task Forces
- Stop.Think.Connect. Campaign

Cyber Fact Sheet

Learn how the FBI is working to address cyber-based threats to national security.
Details | **Story**

Online Predators



The FBI's online predator and child exploitation investigations are now managed under the Violent Crimes Against Children program. **Details**

Cyber's Most Wanted

Artem Semenov
Conspiracy to commit bank fraud

Peteris Sahurovs
Unauthorized access to protected computer; wire fraud

More

OUTERNET

EARN CONNECT EXPERIENCE LEARN GET LIGHTHOUSE

ENABLING UNIVERSAL INFORMATION ACCESS

LIBRARIES FROM SPACE

SEE THE WAYS OUTERNET WORKS

For 80% of humanity, the Internet as we know it does not exist, so we built a new way to share information.


IS IT SAFE?