



# Defining Cyberviolence:

in relation to gender stereotypes and  
violence against women

GARETH SANSOM (CRIMINAL LAW POLICY SECTION, DEPT. JUSTICE CANADA)

T-CY WORKING GROUP ON CYBERBULLYING AND OTHER FORMS OF ONLINE VIOLENCE, ESPECIALLY AGAINST WOMEN AND CHILDREN

“TACKLING GENDER STEREOTYPES AND SEXISM”

28-29 MARCH 2019

HELSINKI, FINLAND

# Cyberviolence: mapping the problem

- ▶ A variety of different terms were used in the academic literature:
  - ▶ Example: “Technology-facilitated sexual violence and harassment” (Henry & Powell 2015); “*Forms of Technology-facilitated Sexual Violence and University Women’s Psychological Functioning*”. (Cripps 2016)
  - ▶ But “technology-facilitated” too broad (ranges from cameras to submachine guns)
  - ▶ More precise focus: Information and communication technologies = ICTs: “ICT-facilitated” and/or “ICT-related”
  - ▶ Analysis goes beyond familiar “content crimes”
  - ▶ Growing body of empirical and sociological studies by academics, NGOs, multilateral and governmental organizations
  - ▶ Age is a significant dimension: children, youth, adult
  - ▶ Gender is a significant dimension: victims and perpetrators

# Cyberviolence: Working Definition

- ▶ The group proposed the following definition for the purpose of the study:
  - **Cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities**
- ▶ **Note: This definition is an adaptation of the definition of “violence against women” in Article 3 Istanbul Convention.**

# Types of cyberviolence

Mapping study revealed there is not yet a stable lexicon or typology of offences considered to be cyberviolence, and many of the examples of types of cyberviolence are interconnected or overlapping or consist of a combination of acts.

## ICT-related violations of privacy

- Computer intrusions
- Taking, sharing, manipulation of data or images, incl. intimate data
- Revenge porn
- Stalking
- Doxing
- Identity theft
- Impersonation
- Etc.

## ICT-related hate crime

Against groups based on

- race
- ethnicity
- religion
- sex
- sexual orientation
- disability
- etc.

## Cyberharassment

- Defamation and other damage to reputation
- Cyberbullying
- Threats of violence, incl. sexual violence
- Coercion
- Insults or threats
- Incitement to violence
- Sextortion
- Incitement to suicide or self-harm
- Etc.

## ICT-related direct threats of or actual violence

- Murder
- Kidnapping
- Sexual violence
- Rape
- Torture
- Extortion
- Blackmail
- Swatting
- Incitement to violence
- Transmissions that themselves cause injuries
- Attacks on critical infrastructure, cars or medical devices
- Etc.

## Cybercrime

- Illegal access
- Illegal interception
- Data interference
- System interference
- Computer-related forgery
- Computer-related fraud
- Child pornography

## Online sexual exploitation and sexual abuse of children

- Sexual abuse
- Child prostitution
- Child pornography
- Corruption of children
- Solicitation of children for sexual purposes
- Sexual abuse via livestreaming
- Etc.

# Example #1:

## Cyberstalking: Intimate Partner Risks

“Contrary to popular misconceptions, research shows that the majority of stalking is perpetrated not by strangers or acquaintances but by intimate partners or ex-partners ... Evidence demonstrates that men are the main perpetrators of intimate partner stalking, both in Australia and internationally .... Reviews of international research demonstrates that women are more likely to be stalked than men ... and are more likely to experience fear due to stalking.” (Woodlock 2017: 584-585)

- ▶ Typical: **Coercive control of daily behaviours**; persistent texting, email; tracking partners' location via GPS or IoT; control of female partner's computer (for surveillance of communication)
- ▶ Stalking by intimate partners can be persistent and dangerous: Woodlock (2017: 586) cites a national U.S. survey that “found that cases involving intimate partners lasted 2.2 years on average, compared with 1.1 years for stalking by others”
- ▶ Intimate partner stalking more likely to be associated with homicides and attempted homicides than stalking by strangers
- ▶ Delanie Woodlock. “The Abuse of Technology in Domestic Violence and Stalking” (2017)

# Example #2:

## Cyberbullying and the Social Self

- ▶ Transformation of contemporary life – smart phones, social media, blogs, “selfies”, documenting and sharing every-day behavior – including intimate behavior - particularly among youth
- ▶ Construction of the self, of identity, of gender (through lived relations as well as through prevalent gender stereotypes and cultural or subcultural ideals)
- ▶ Perception and self-perception of one’s own body; and one’s own lived experience: what is specific relation between the embodied and the disembodied within the given peer group;
- ▶ Identity can be fluid but it can also be rigid and brittle (avoid generalizations)
- ▶ New technologies (video games, virtual reality, self-generated content) can permit exploration of the range of identities, including gendered identities – in some cases this can be liberating, in others oppressive and frightening

# Ways of Understanding Some Aspects of the Phenomenon

- ▶ Technologies as **practices of constructing the self** and “**extensions**” of the self
- ▶ The self is not bounded by the physical body but extends into social media: one’s own images, both held “privately” and in shared social space, including “cyberspace” and other ICT-mediated spaces
- ▶ This “digital archive” can become part of the self and can be a crucial aspect of one’s identity as well as mediators with the other (especially peer groups)
- ▶ Attacks on the digital archive can be experienced as attacks on the self
- ▶ Peer groups have always been important in the formation of identity but they can also bring about the “destruction” of identity and can lead to or even promote self-harm; range of circumstances: betrayal by family, by friends, shame, etc.
- ▶ In addition there is also a **distinct** phenomena which insinuates itself into this new ICT-mediated world: Serial offenders with multiple victims in multiple countries sometimes with sophisticated hacking skills (see Type 3 below)
- ▶ Tragedy of teenage suicides (predominantly teenage girls and young women) – can result from different sets of these circumstances – not just response to peer groups but also triggered by “predatory” actions (coercion, extortion, sustained and severe harassment) by offenders

# Gender stereotypes and Cyberviolence

- ▶ The “Mapping Study” did not specifically focus on gender stereotypes and cyberviolence against women but scholarly and other articles in the literature review occasionally touched on the relationship
- ▶ In the context of this conference, exploring the correlation in its relation to specific online forms of cyberviolence (such as cyberstalking and cyberbullying) may suggest directions for further research
- ▶ An implication of the study is that different types of cyberviolence involve:
  - ▶ Different relations to the technology and computer networks
  - ▶ Different social networks
  - ▶ Different types of perpetrators or instigators of violence



Social scientist as  
“alien ethnographer”

Ji'rar Bai-Tzon  
of the  
Great Race of Yith

(from 1930s science fiction writer:  
H.P. Lovecraft)



Image by Vishchun

**Spiral:** Victim feels trapped in centre



A bit like a “**positive feedback loop**”: it just keeps circling round and round

From the field notes of Ji'rar Bai-Tzon

**Category:** Intra-species violence – with gender bias

**Mechanism:** system characterized by positive feedback loops lacking homeostatic correction

Behaviour Type 1	Behaviour Type 2
<b>Local Name:</b> “Cyberstalking”	<b>Local Name:</b> “Cyberbullying”
<b>Environment:</b> ubiquity of ICTs	<b>Environment:</b> ubiquity of ICTs
<b>Modality:</b> reduction of deployed devices in network proximate to Agent B (“victim”) to surveillance monitors and/or behavioural conditioning prods (series of violations of fundamental right to privacy) <b>Example:</b> Internet of Things to create “tracking grid”	<b>Modality:</b> “software” extensions of agents into fractal, distributed archives of “self” with vector instability (local slang: “social media network”)
<b>Social structure:</b> intimate partners	<b>Social structure:</b> peer group (potentially with intimate partner dyads or other combinants)
<b>Potential System Outcome:</b> homicide (Agent B)	<b>Potential System Outcome:</b> suicide (the “third”)


From the field notes of Ji'rar Bai-Tzon

Behaviour Type 1	Behaviour Type 2
<b>Local Name: “Cyberstalking”</b>	<b>Local Name: “Cyberbullying”</b>
<b>System: <i>Asymmetrical</i> schismogenesis between agents acting as “unequals”</b>	<b>System: <i>Symmetrical</i> schismogenesis between agents acting as “equals” (“peer group”)</b>
<b>Feedback loop: cycle of increased non-consensual dominant behaviour (of Agent A) elicits submissive behaviour (of Agent B)</b>	<b>Feedback loop:</b> (within peer group): response to assertive behaviour is more assertive behaviour (or cohort approval by replication of assertive behaviour) (indigenous slang: <i>See “dissing”; “re-tweets”, “going viral” etc.</i> )
<b>Unique factor: possible state of ethically non-viable homeostasis, breakdown of dyad, or physical cessation of Agent B</b>	<b>Unique factor:</b> mimetic desire among peers generates (leads to emergence of) a “third” (indigenous historical term: “scapegoat”); social system elicits exclusion of “third” from peer group: aggravating factor: non-consensual distribution of intimate images
<b>Logic (Agent A): “incorporation” (encyst, then consume and/or destroy)</b>	<b>Logic(peer group):</b> social exclusion (indigenous historical ritual: physical sacrifice of the scapegoat)

## Preliminary suggestions for further research

<b>Gender Stereotypes in specific contexts</b>	
<b>Behaviour Type 1</b>	<b>Behaviour Type 2</b>
<b>Local Name: “Cyberstalking”</b>	<b>Local Name: “Cyberbullying”</b>
<b>Imposition by Agent A of gender stereotypes Male= Dominant &amp; Female = Submissive (regardless of or in opposition to Agent B’s views)</b>	<b>Status within the peer group is linked to either proximity to or advocacy of gender-based image ideals</b>
<b>Note: This behaviour is non-consensual; it is not a “role play game” or “fantasy as play”: it is a relation of power</b>	<b>Note: Empirical study of specific peer groups essential: what are the “image ideals” sustaining mimetic desire within a specific peer group? How is male and female constructed ? Inflections of gender stereotypes by class, ethnicity, religion may distinguish between peer groups?</b>
<b>Potential shift in gender stereotypes of Agent B following sustained behavioural conditioning: Consider spectrum: “Virtual” confinement through to physical confinement (“girl in the box” – example: Stan, 1977-1984)</b>	<b>Is membership in the peer group gender exclusive and/or restricted by sexual orientation (is the peer group male-only, female-only, heterosexual-only, etc.)</b>
	<b>Is membership in peer group based on real or imagined disenfranchisement (perception of loss of power)?</b>

From the field notes of Ji'rar Bai-Tzon

Behaviour Type 3	
Compound/Hybrid Behaviour Type 1 subsumes Behaviour Type 2	
Local Name: "Cyberbullying"	
<b>Instigator/Perpetrator</b> 	<b>Triggers</b> Scapegoating within peer group
<b>System:</b> <i>Asymmetrical</i> schismogenesis between agents acting as "unequals"	<b>System:</b> <i>Symmetrical</i> schismogenesis between agents acting as "equals" ("peer group")
<b>Feedback loop:</b> cycle of increased non-consensual dominant behaviour (of Agent A) elicits submissive behaviour (of Agent B)	<b>Feedback loop:</b> (within peer group): response to assertive behaviour is more assertive behaviour (i.e., cohort approval by replication of assertive behaviour)
<b>Unique factor:</b> serial perpetrator – outside peer group	<b>Unique factor:</b> contagion of mimetic desire shifts toward social violence directed at Agent B
<b>Logic (Agent A):</b> power/control, sadism	<b>Logic</b> (peer group): social exclusion

# Other diverse phenomena referenced in report

- ▶ Use of ICTs to coordinate ethnically and racially motivated attacks and sexual assaults
- ▶ Recording of rape and gang rape by youth and young men, followed by distribution of videos through a range of channels
- ▶ “Real world” harm: direct use of ICTs to inflict harm (example: malware to purposely trigger epileptic seizures)
- ▶ Has given rise to a new vocabulary: “sexting”, “doxing”, “Swatting”, “sextortion”, “revenge porn”

Orienting  
further  
discussion

**Budapest Convention  
on Cybercrime**

Substantive  
cybercrime  
offences

Procedural  
Powers:  
collection of  
digital evidence

international  
cooperation  
in criminal  
Justice (MLA, etc.)

**“Lanzarote” Convention** on the  
Protection of Children against Sexual Exploitation  
and Sexual Abuse (CETS 201)

**Istanbul Convention.**  
“Council of Europe Convention on  
preventing and combating violence against  
women and domestic violence” (CETS 210)