Offline and Local: The Hidden Face of Cybercrime
Background

• Cybercrime is a largely anonymous activity that exists in cyberspace (see Grabosky, 2004; Wall, 2007; Lusthaus, 2013).


• Shadowy attackers could strike from anywhere at any moment.

• A new type of threat...
Offline/Local Dimension

- Highlighting a neglected aspect of the cybercrime phenomenon: the offline and local dimension.
- All cyber-attacks stem from a person who physically exists in a certain location.
- Expect a degree of variation as to how cybercrime presents in each case based on socio-economic factors.
- Both the individuals behind cybercrime and the offline worlds they inhabit deserve study.
- Alongside the online and technical, there is an offline, human and contextual element that matters.
Approach and Methods

• Case study of Romania (a leading cybercrime hub), as an exploratory pilot study.
• 2 fieldwork visits Sep 2014 & March 2015 to Bucharest, Ramnicu Valcea and Alexandria.
• Field observations and semi-structured interviews.
• 17 participants: LE, private sector, a journalist, a hacker, a former cybercriminal and more...
The Local Brand

- ‘Online auction fraud’ is a Romanian speciality, with a traditional focus on fictitious cars.
- Began with eBay, but has now migrated to other platforms as well.
- Multimillion dollar business (Hall, 2014; Odobescu, 2014).
- Scams often target the West, but developing countries now also targeted (LV2).
Why Romania?

- Legacy of communism:
  - Ceausescu invests in education and reverse engineering computers is important (Heeks and Grundey, 2004; LV10; LV11).
  - Romanians are successful internationally, foreign companies operate in Romania, along with startups (LV1; see Coleman, 2014).
  - Micro-networks and Internet pioneers, good connectivity.
Why Romania 2

• The infrastructure exists for fast and successful online (criminal) operations.
• May explain why online fraud rather than hacking/malware is the Romanian cybercrime par excellence (technical players are employed).
Why Romania 3

• Economic situation is relatively poor despite the IT situation (2014 average salary is 398 euros a month - the EU average is 1,489).

• Corruption remains high in Romania (TI 2016 Corruption Perceptions Index, Romania scores 48 out of a possible 100).

• Scams are around...

• A fertile environment for online fraud?
Number of decisions of the Court of Appeals for cases involving ‘fraudă informatică’, 2008-2010, Romania (Source: Juridex)

<table>
<thead>
<tr>
<th>Region</th>
<th>Number of cases</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA PITEȘTI</td>
<td>75</td>
<td>26.98</td>
</tr>
<tr>
<td>CA BUCUREȘTI</td>
<td>38</td>
<td>13.67</td>
</tr>
<tr>
<td>CA BACĂU</td>
<td>25</td>
<td>8.99</td>
</tr>
<tr>
<td>CA CLUJ</td>
<td>22</td>
<td>7.91</td>
</tr>
<tr>
<td>CA BRAȘOV</td>
<td>21</td>
<td>7.55</td>
</tr>
<tr>
<td>CA CRAIOVA</td>
<td>19</td>
<td>6.83</td>
</tr>
<tr>
<td>CA ALBA IULIA</td>
<td>18</td>
<td>6.47</td>
</tr>
<tr>
<td>CA GALAȚI</td>
<td>16</td>
<td>5.76</td>
</tr>
<tr>
<td>CA TIMIȘOARA</td>
<td>11</td>
<td>3.96</td>
</tr>
<tr>
<td>CA IAȘI</td>
<td>10</td>
<td>3.60</td>
</tr>
<tr>
<td>CA CONSTANȚA</td>
<td>9</td>
<td>3.24</td>
</tr>
<tr>
<td>CA PLOIEȘTI</td>
<td>9</td>
<td>3.24</td>
</tr>
<tr>
<td>CA SUCEAVA</td>
<td>4</td>
<td>1.44</td>
</tr>
<tr>
<td>CA ORADEA</td>
<td>1</td>
<td>0.36</td>
</tr>
<tr>
<td>CA TG MUREȘ</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CA MILITARĂ</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TR VRANCEA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>278</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>
The Regional Story

• Ramnicu Valcea (aka ‘Hackerville’) is a major hub of cybercrime, though its nickname should be ‘Fraudville’.
• Local specialty is auction fraud, the major industry.
• Cafes, shops, malls, shiny black luxury cars...
• Few other sources of wealth: OltChim plant struggles/becomes insolvent in 2013.
• Many believe this is a cybercrime hub (Wylie, 2007; Bhattacharjee, 2011; Bran, 2011; Hall, 2014; see also Wittkop, 2016, pp. 163–164).
Organisation

• Two components:

1) Organisation of fraud (coordinated team advertising fake products/engaging customers)

2) “Arrows” (money mules moving money back from UK/US etc – money transfer agencies and more)

• In both cases, many offenders know each other personally...
Organisation 2

"I don’t know if the people of Ramnicu Valcea are too smart or too stupid... They talk a lot to each other. One guy learns the job from another. They ask their school friends: Hey, do you want to make some money? I want to use you as an arrow. Then the arrow learns to do the scams himself.” (Bhattacharjee 2011)
The Very Local Dimension

• According to local prosecutors, mostly based in the Ostroveni neighbourhood (Bran, 2011).
• Allegedly, High School no. 10 is a focal point.
• But many scammers have now grown up.
• Parallels to ‘network effects’ of expertise and knowledge in legitimate industry (Reagans and McEvily, 2003).
Corruption/Protection

- Corruption appears to aid cybercrime:
  - Deputy Head of Ramnicu Valcea police arrested in December 2014 for revealing confidential information to criminals.
  - March 2015, another police officer arrested for passing information to a cyber fraud group (Ripan, 2015).
  - Socialist senator implicated in another case with a violent criminal (Miercuri, 2015).
Conclusion

• Cybercrime has important offline and local dimensions, alongside the online component.
• Large-scale cybercrime can thrive thanks to offline social networks.
• These points do not relate only to the case of Romania (see, for instance, Lusthaus, 2016, pp. 24–31; Leukfeldt, 2014; Leukfeldt et al., 2016).
Conclusion 2


• Organized criminal enterprises are ‘local in scope’ (Reuter, 1985, p. 21; Gambetta 1993).

• Cybercrime needs to be tackled in the places where it originates.

• Romanian model as a way forward?