What is **Virtual Forum against Cybercrime**?

An internet platform to share information on cybercrime and to train law enforcement and judicial officials in fighting cybercrime.

- **Online Training Program**
  Technical assistance in Asian countries through training and education

- **Research Network**
  “One-stop shop” for cybercrime experts and specialists worldwide
Cybercrime

- is borderless, transnational crime
- spreading throughout the world
- is ubiquitous, a part of daily life
- threatening safety of society and international security
Emanated from the 11th UN Congress on Crime Prevention & Criminal Justice in Bangkok (2005)

Proposed by the United Nations Office on Drugs & Crime (UNODC) and the Korean Institute of Criminology (KIC)

Five international expert group meetings were held to discuss the development of the Virtual Forum against Cybercrime (2006 to 2008)
DEVELOPMENT OF VFAC

- Aug. 2010: Official Open of the Research Network
- Sep. 2009: Organized 5 international expert group meetings
- 2006-2008: Recommended during the 11th UN Congress on CCPCJ
- Apr. 2005: Official Launch of the Online Training Program
“Clearinghouse” of research resources on cybercrime

Research Network comprises:

- News & Trends
- Statistics & Surveys
- Publications
- Professionals
- Institutions and Organizations
- Legislation
- Discussion Group

... created, updated and improved with the assistance of experts around the world through international cooperation
## News & Trends

<table>
<thead>
<tr>
<th>No</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oracle gives word of upcoming fixes</td>
<td>2011-01-14</td>
</tr>
<tr>
<td>2</td>
<td>IT managers urged to tighten mobile security policies</td>
<td>2011-01-14</td>
</tr>
<tr>
<td>3</td>
<td>Popular institutional websites hijacked</td>
<td>2011-01-14</td>
</tr>
<tr>
<td>4</td>
<td>Alexa's top one-million showcases malicious domains</td>
<td>2011-01-13</td>
</tr>
<tr>
<td>5</td>
<td>Microsoft offers temporary Internet Explorer fix</td>
<td>2011-01-12</td>
</tr>
<tr>
<td>6</td>
<td>Cyberwarfare Roshanbo: th3J2542r Profited</td>
<td>2011-01-12</td>
</tr>
<tr>
<td>7</td>
<td>Network security spending to soar over next five years</td>
<td>2011-01-11</td>
</tr>
<tr>
<td>8</td>
<td>Spam back on track with UK in fifth place</td>
<td>2011-01-11</td>
</tr>
<tr>
<td>9</td>
<td>Amazon cloud enables wireless hacks</td>
<td>2011-01-10</td>
</tr>
<tr>
<td>10</td>
<td>Security experts warn of PayPal phishing scam</td>
<td>2011-01-10</td>
</tr>
<tr>
<td>11</td>
<td>Android trojan sign of mobile malware evolution</td>
<td>2011-01-10</td>
</tr>
<tr>
<td>12</td>
<td>US authorities subpoena Twitter for WikiLeaks data</td>
<td>2011-01-08</td>
</tr>
<tr>
<td>13</td>
<td>Malware creation goes off the scale in 2010</td>
<td>2011-01-05</td>
</tr>
<tr>
<td>14</td>
<td>McAfee warns of more WikiLeaks-style hackivist attacks</td>
<td>2011-01-04</td>
</tr>
<tr>
<td>15</td>
<td>Microsoft and Google dash over zero-day flaw release</td>
<td>2011-01-04</td>
</tr>
<tr>
<td>16</td>
<td>Pro-WikiLeaks hackers take aim at government sites</td>
<td>2011-01-04</td>
</tr>
<tr>
<td>17</td>
<td>DHS zeroing in on Vietnamese-based fraud ring</td>
<td>2011-01-04</td>
</tr>
<tr>
<td>18</td>
<td>Is the Storm Worm botnet trying to make a 2011 comeback?</td>
<td>2011-01-03</td>
</tr>
<tr>
<td>19</td>
<td>IBM predicts rising mobile threats, critical infrastructure attacks in 2011</td>
<td>2011-01-03</td>
</tr>
<tr>
<td>20</td>
<td>Anonymous targets corrupt Zimbabwe government</td>
<td>2010-12-30</td>
</tr>
</tbody>
</table>
“Online Classroom” about cybercrime

Accessible anywhere with computer and Internet

designed for the law enforcement and judicial officials

Consists of five modules with 130-hour lessons and topics

Five modules, 130 hours

1) Understanding Information and Communication Technology
2) Understanding Cybercrime Laws
3) Cybercrime Investigations - Procedure & Techniques
4) Cybercrime Investigations - Digital Forensics
5) Special Online-Seminars-Issues and Topics
A. Introductory Course

[1] Understanding Information and communication Technology

- Structure of the Internet & Digital Divide
- ICT & network security
- E-commerce & forms of electronic payment
- Digital Evidence & Digital Forensics for non-forensic specialists
[2] Understanding Cyberspace Laws

- Criminality – Definitions of cybercrime
- Types of Cybercrimes and laws (I-V) – Cyber-violence, cyber-property crimes, e-commerce & e-banking crimes, cyber-terrorism
- Jurisdiction – the roles of national & international law enforcement
B. Advanced Courses for Specialists

- [3] Cybercrime Investigations – Procedure & Techniques
  - Computer investigation techniques
  - Investigation system & procedure of advanced countries
  - Criminal procedure & digital evidence
  - Modus Operandi of Cybercrime & investigation technique: hacking & botnet, etc.

- Understanding and applying the rules of digital evidence
- Acquiring forensic images and preservation of digital evidence
- Analytical procedures and forensic techniques
Online Training

- Data Protection
- Online Gambling
- ID Theft & Online Fraud

Special Issues and Topics

- Cybercrime Investigation
- Procedures and Techniques
- Digital Forensic

- Cybercrime Law
- Information & Communication Techniques
- Introduction to this Online Training Program

85 lessons

- 2 month course

- 6 month course

- 20 lessons
- Special Issues and Topics
- Data Protection
- Online Gambling
- ID Theft & Online Fraud

- Advanced

- Introductory
Sample Course

**MISSING CONTROL**

- Internet was developed as a military network
- Consequences
  - Strategic and military aspects dominated the development of the technology - not the needs of a global mass communication network
- Resistant against nearly any form of centralised control
- Major consequences
  - Independence of place of action and place of the result
  - International Dimension
www.cybercrimeforum.org

Contact point

onlinetraining@kic.re.kr
Thank You!

www.kic.re.kr / www.cybercrimeforum.org