BOOM! HEADSHOT!

or…Cheating and Subliminal Exploitation in Combat Simulations and Online Gaming

Mike Bond

Computer Security Group, University of Cambridge CL, 1st Jun 07

(first presentedSecurity and Protection of Information 2007, Brno)

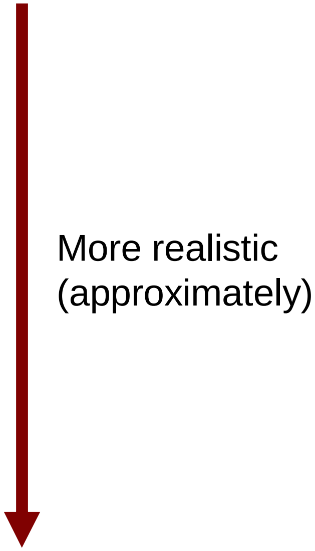
Talk Overview

- Online Games and Combat Sims
- Why Security Matters in Gaming
- Tactics & Security Taxonomy
- Existing Knowledge Survey
  - Unintentional glitches
  - Glitches, exploits, cheats
- New Topic: Subliminal Exploits
- Studying Online Gaming

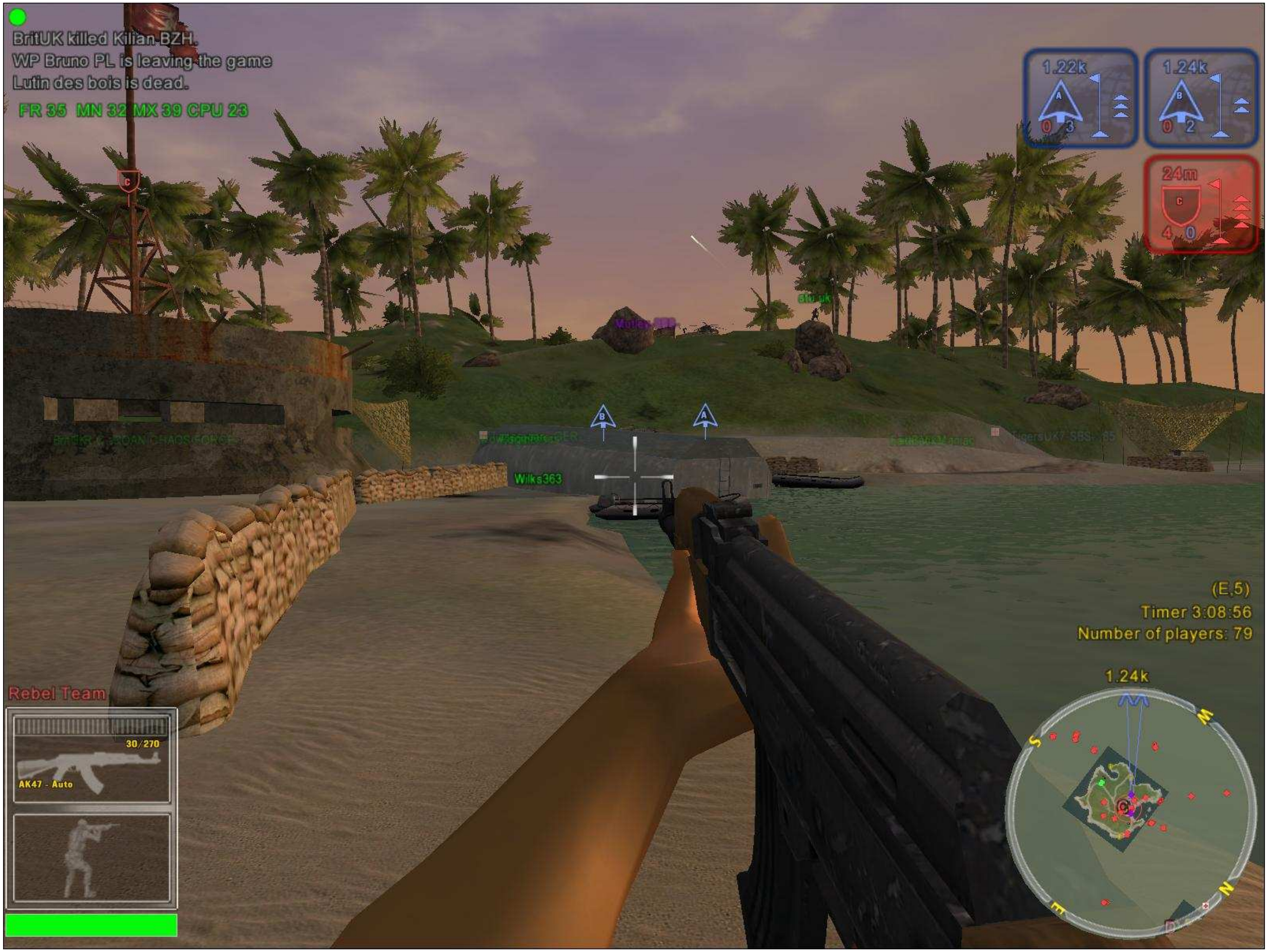
Games and Combat Sims

- Multi-player, online, team-based combat

- Counterstrike (Valve, Half-Life Mod)
- Battlefield 2 (EA Dice)
- Joint Operations (Novalogic)
- America’s Army (US DOD)
- Operation Flashpoint (BIS)
- Armed Assault (BIS)



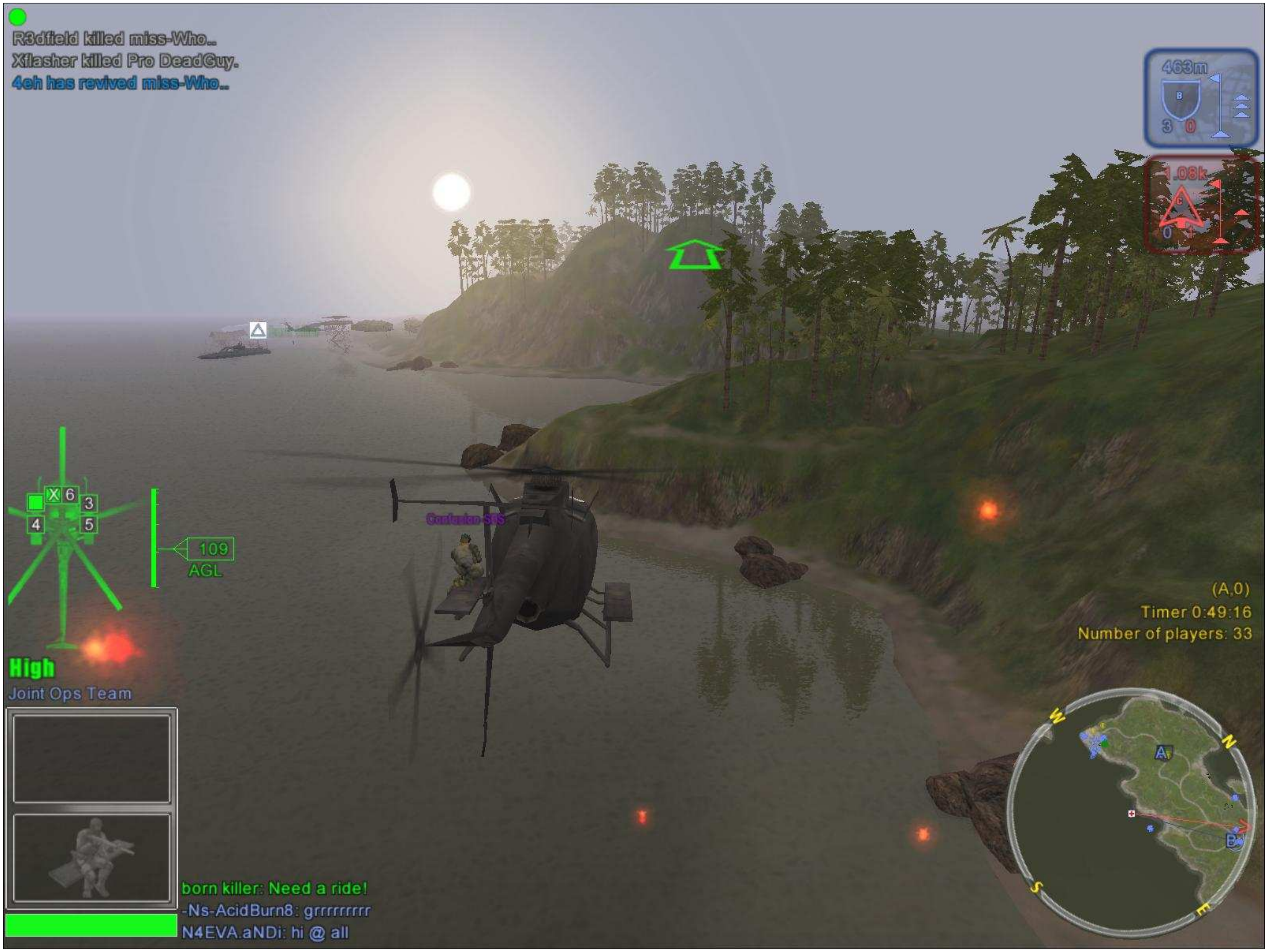
Joint Operations



BritUK killed Kilian BZH.
WP Bruno PL is leaving the game
Lutin des bois is dead.
FR 35 MN 32 MX 39 CPU 23

(E,5)
Timer 3:08:56
Number of players: 79

Joint Operations (2)

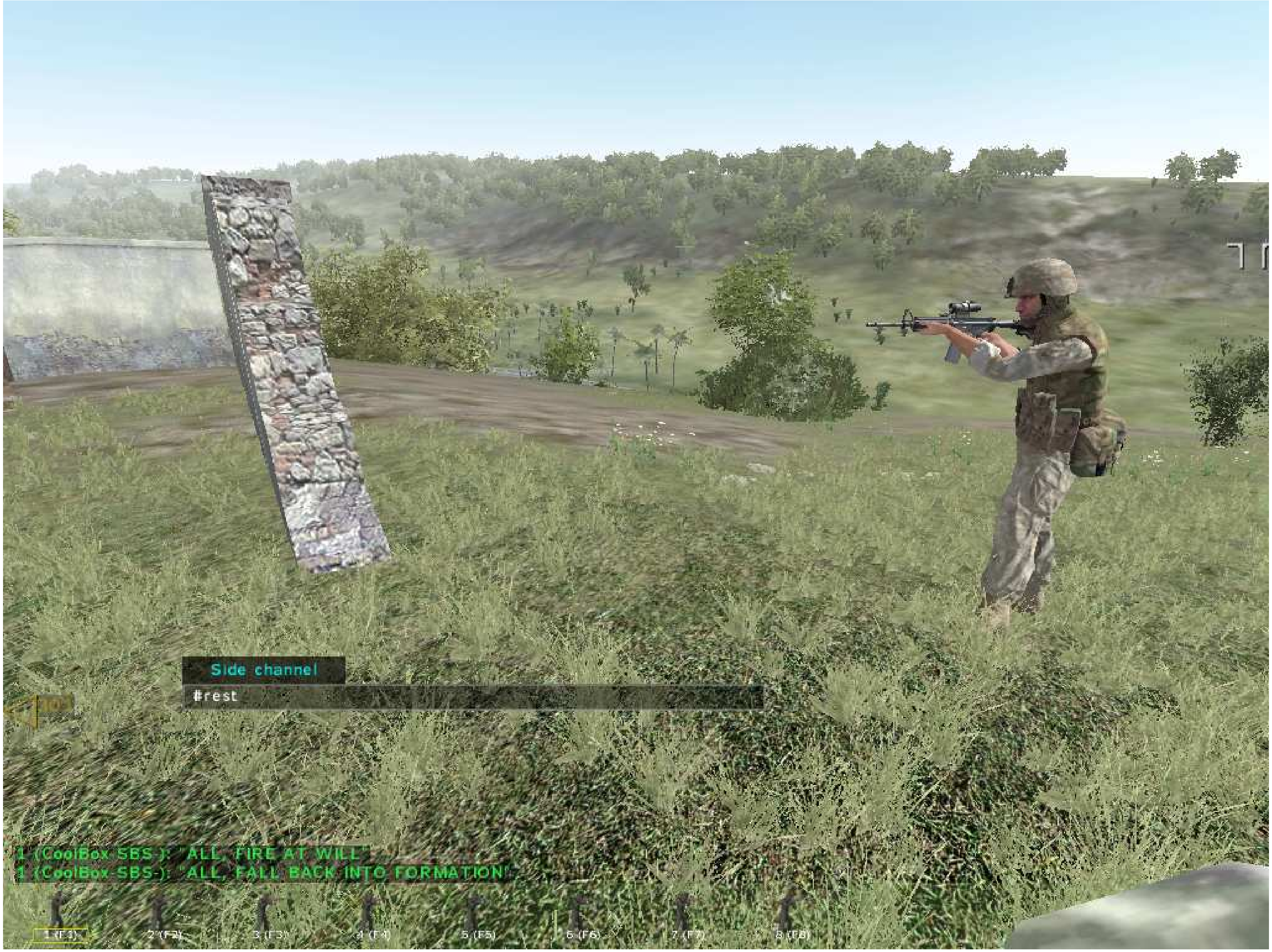


R3dfield killed miss-Who..
Xflasher killed Pro DeadGuy.
4eh has revived miss-Who..

(A,0)
Timer 0:49:16
Number of players: 33

born killer: Need a ride!
-Ns-AcidBurn8: grrrrrrrrr
N4EVA.aNDi: hi @ all

Armed Assault

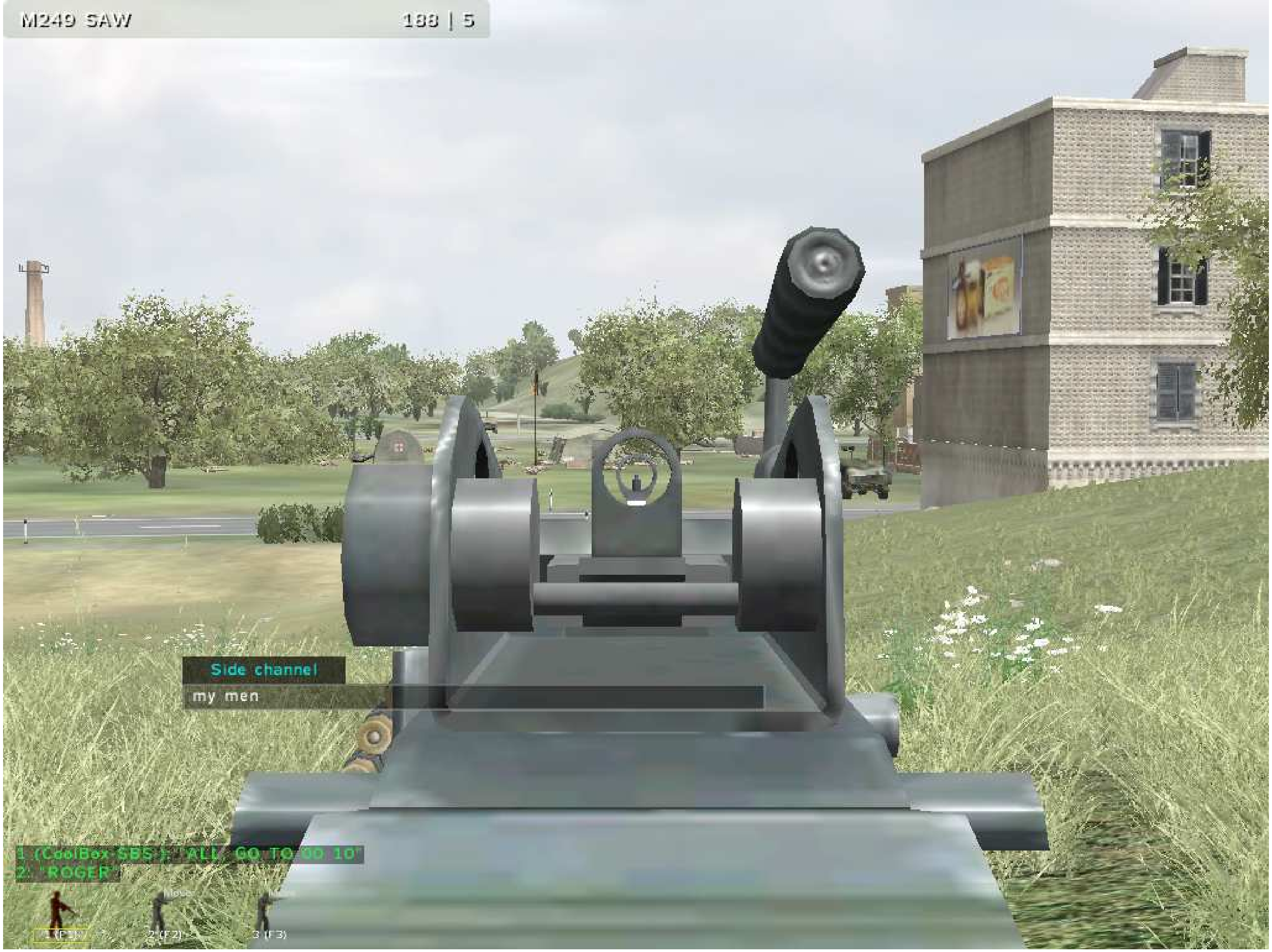


Side channel

#rest

1 (CoolBox-SBS-): "ALL, FIRE AT WILL"
1 (CoolBox-SBS-): "ALL, FALL BACK INTO FORMATION"

Armed Assault (2)



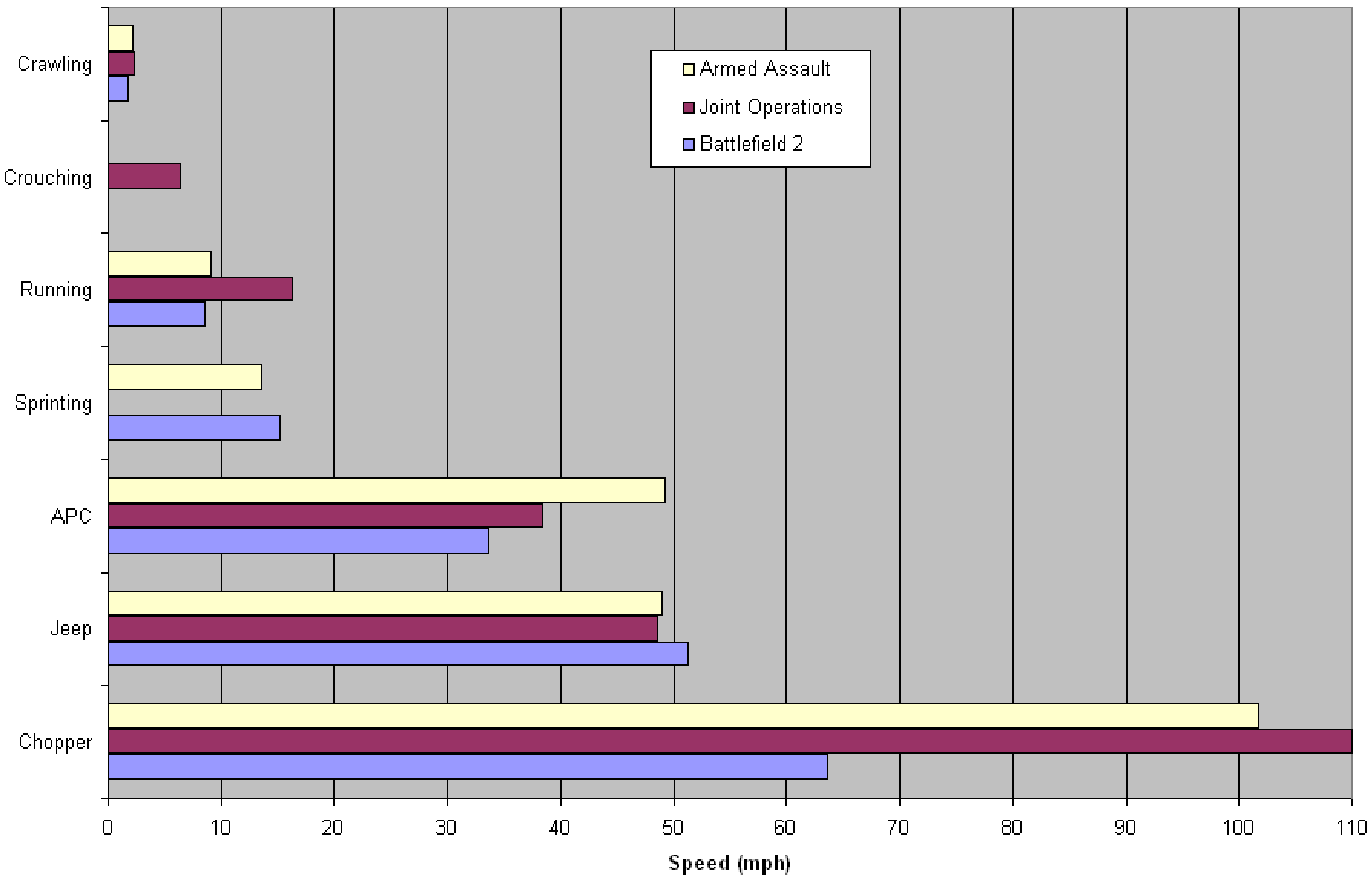
my men

1 (CoolBox SBS): "ALL, GO TO 00 10"
2: "ROGER"

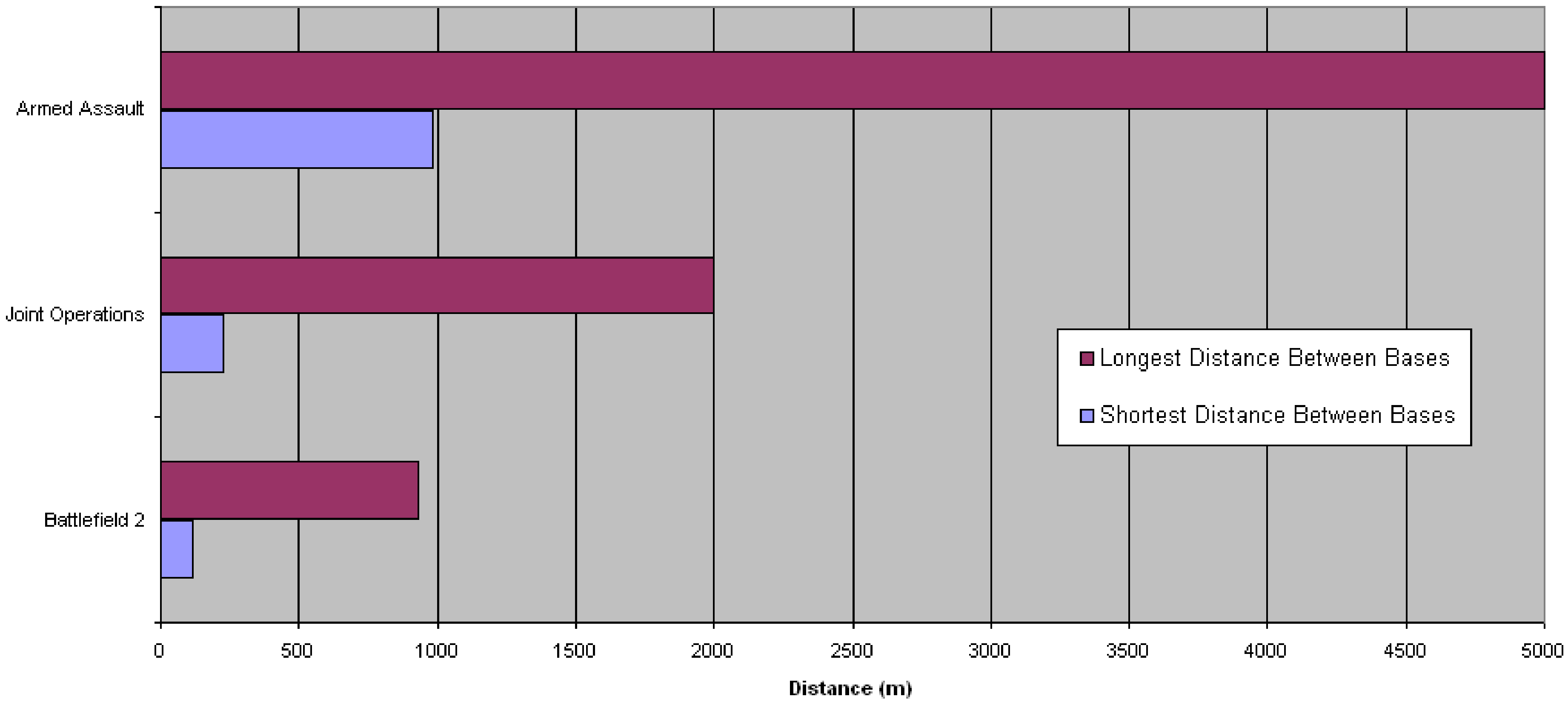
Arcade versus Tactical

- Tactical Shooters
  - World simulation more accurate: players, scale, weather, tides
  - Not about who shoots first, but who sees who first.
  - No (accurate) firing on the move
  - Realistic damage (one shot can kill, immobilising/debilitating wounds)
  - Value of life greater (no respawn/revival)
  - Mobility and logistics as important as combat
- Overall goal: success in a tactical shooter relies on real world tactics, not game mechanics

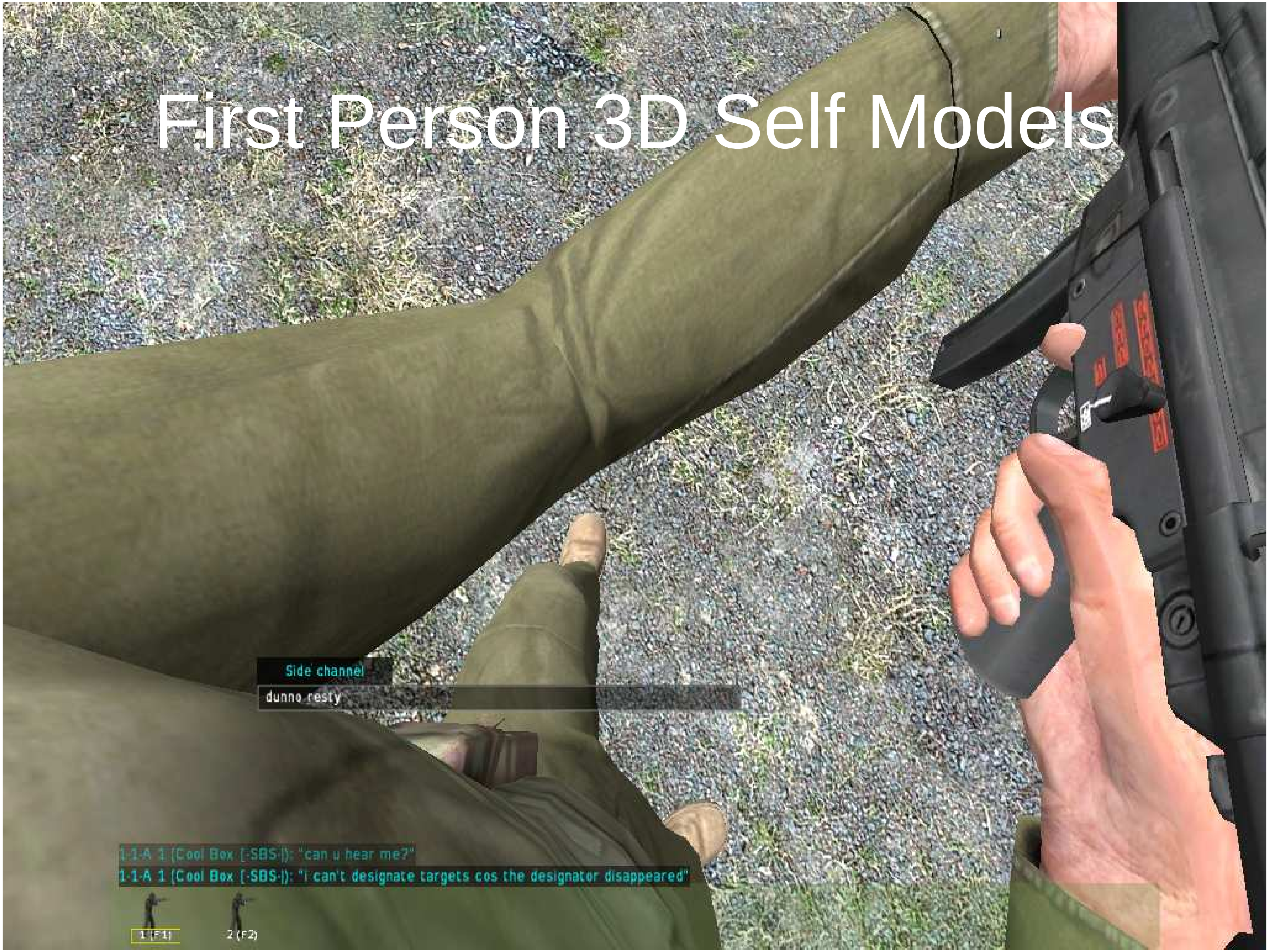
Arcade versus Tactical (2)



Arcade versus Tactical (3)



First Person 3D Self Models



dunno resty

1-1-A 1 (Cool Box [-SBS-]): "can u hear me?"

1-1-A 1 (Cool Box [-SBS-]): "i can't designate targets cos the designator disappeared"

Entertainment Applications

- Single-player story driven
- Single-player arcade
- Multi-player arcade
  - – humans are just used as better AI
- Multi-player team-based
  - – players enjoy+benefit from grouping together
  - – long term groupings form, leagues etc.
  - – 8v8 up to 75v75

Military Applications

- Role-playing Scenarios and Tutoring
  - Remote internet sessions with in-the-field experts training recruits before first deployment
- Combat tactics training
- Logistics training
- Public Relations & Recruiting (America’s Army)
- General Mental Fitness
  - Decision Making, Reactions, Concentration
- Remote Drone Training

Why Cheating Matters to Gamers

- Online gaming is a **sport**
  - Everyone deserves a fair chance, a level playing field – cheating destroys this
- People don’t enjoy an unfair fight
  - Mis-matched boxers = no fun
- **The perception of unfairness/cheating also destroys enjoyment**
- If gamers don’t enjoy it, they don’t stay playing

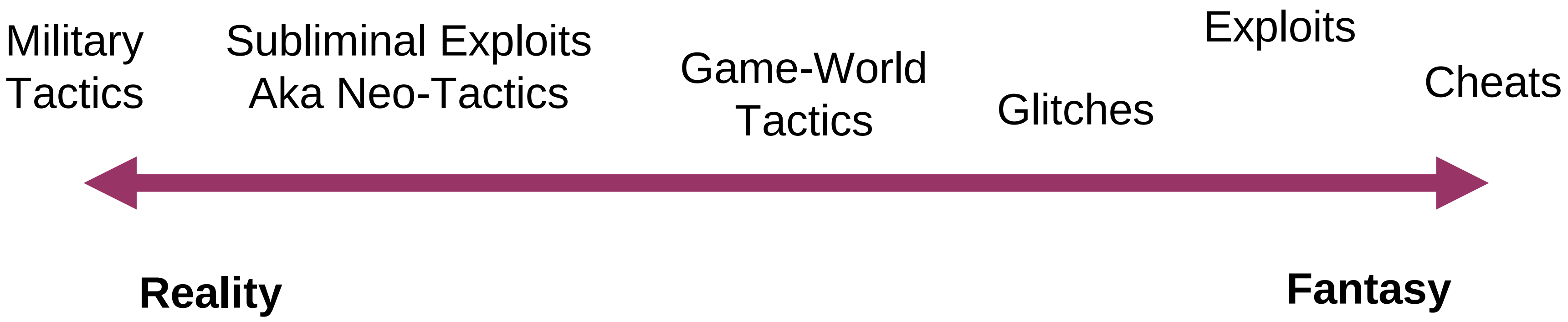
  = no expansion pack sold

  = no monthly subscription paid in (MMOGs)

Could Cheating Matter to the Military?

- Learning the Wrong Lessons
  - Diagnosed (OK… redesign the training to avoid those scenarios)
  - Undiagnosed (Untold, unmeasured damage!)
- Negative PR Image
  - America's Army spreading "US military values" such as cheating / griefing / abuse

Tactics and Security Taxonomy



Military Tactics

Subliminal Exploits Aka Neo-Tactics

Game-World Tactics

Glitches

Exploits

Cheats

Reality

Fantasy

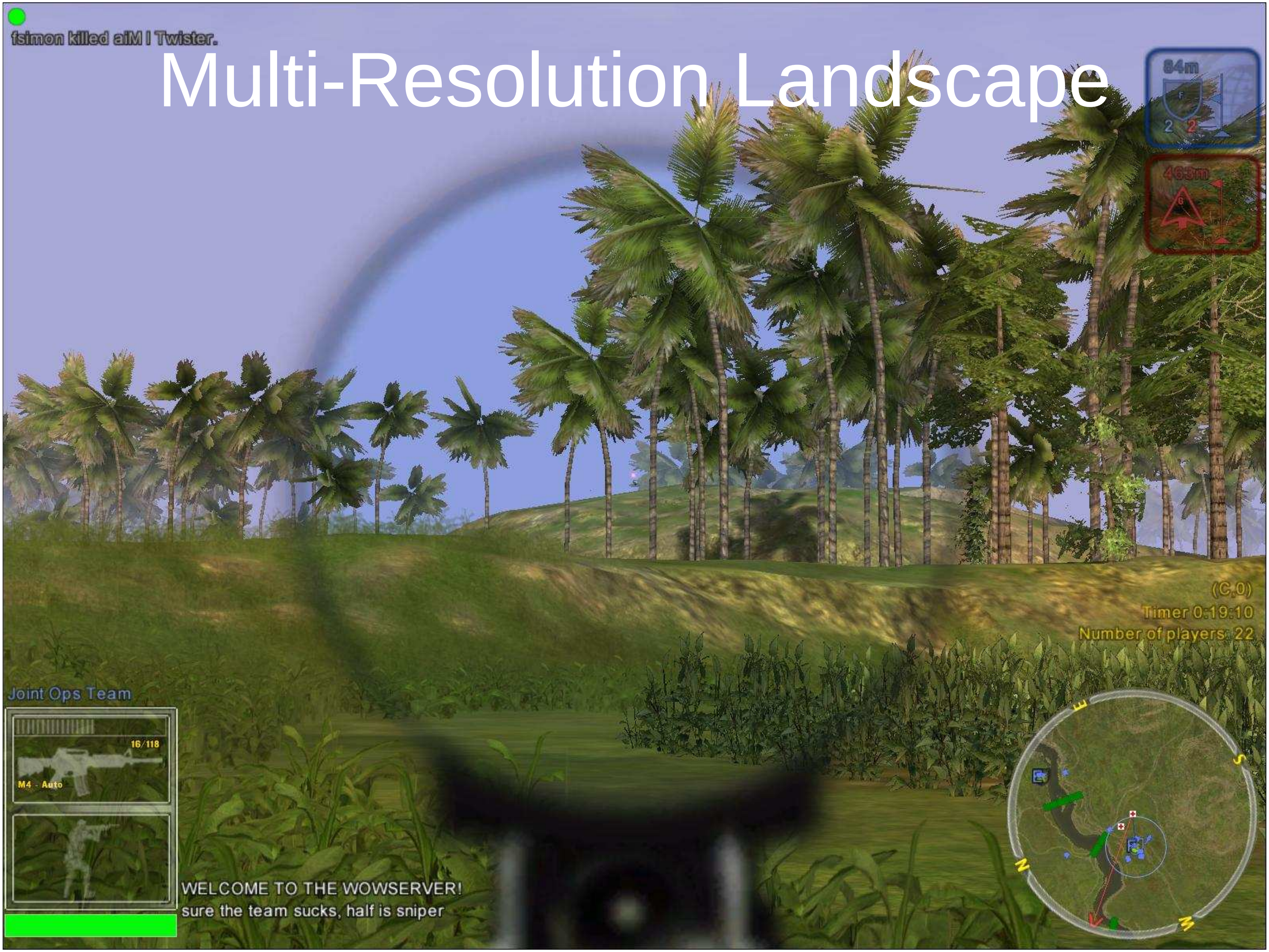
- We’ll look at
  - Unintentional Glitches & Anomalies
  - Deliberate Glitches & Exploits
  - Good Old Fashioned Cheats
  - Subliminal Exploits / Neo-Tactics

Unintentional Glitches and Anomalies

-spoil immersion/fairness

-inspire malicious glitches

Multi-Resolution Landscape

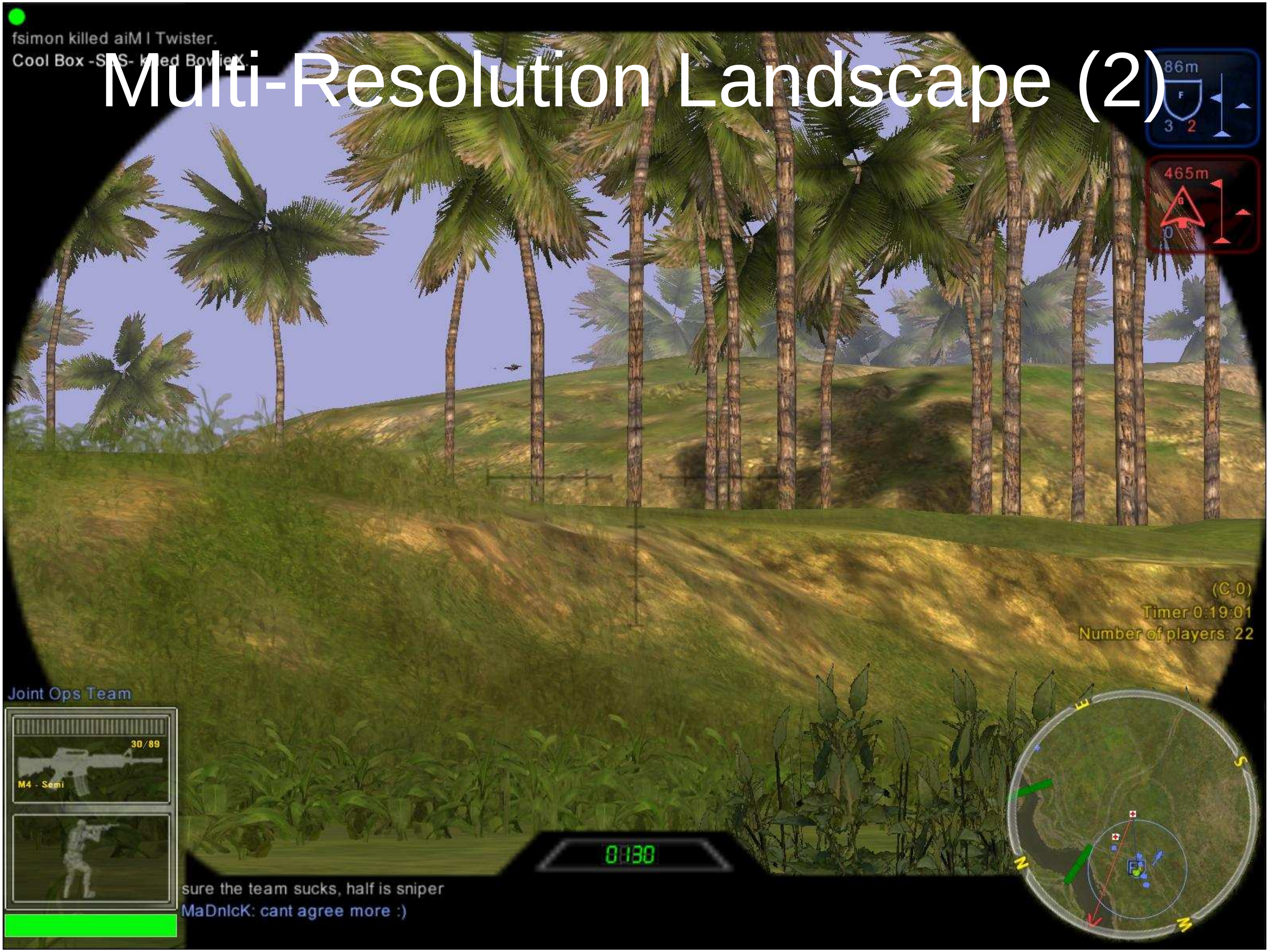


fsimon killed aiM I Twister.

WELCOME TO THE WOWSERVER!

sure the team sucks, half is sniper

Multi-Resolution Landscape (2)



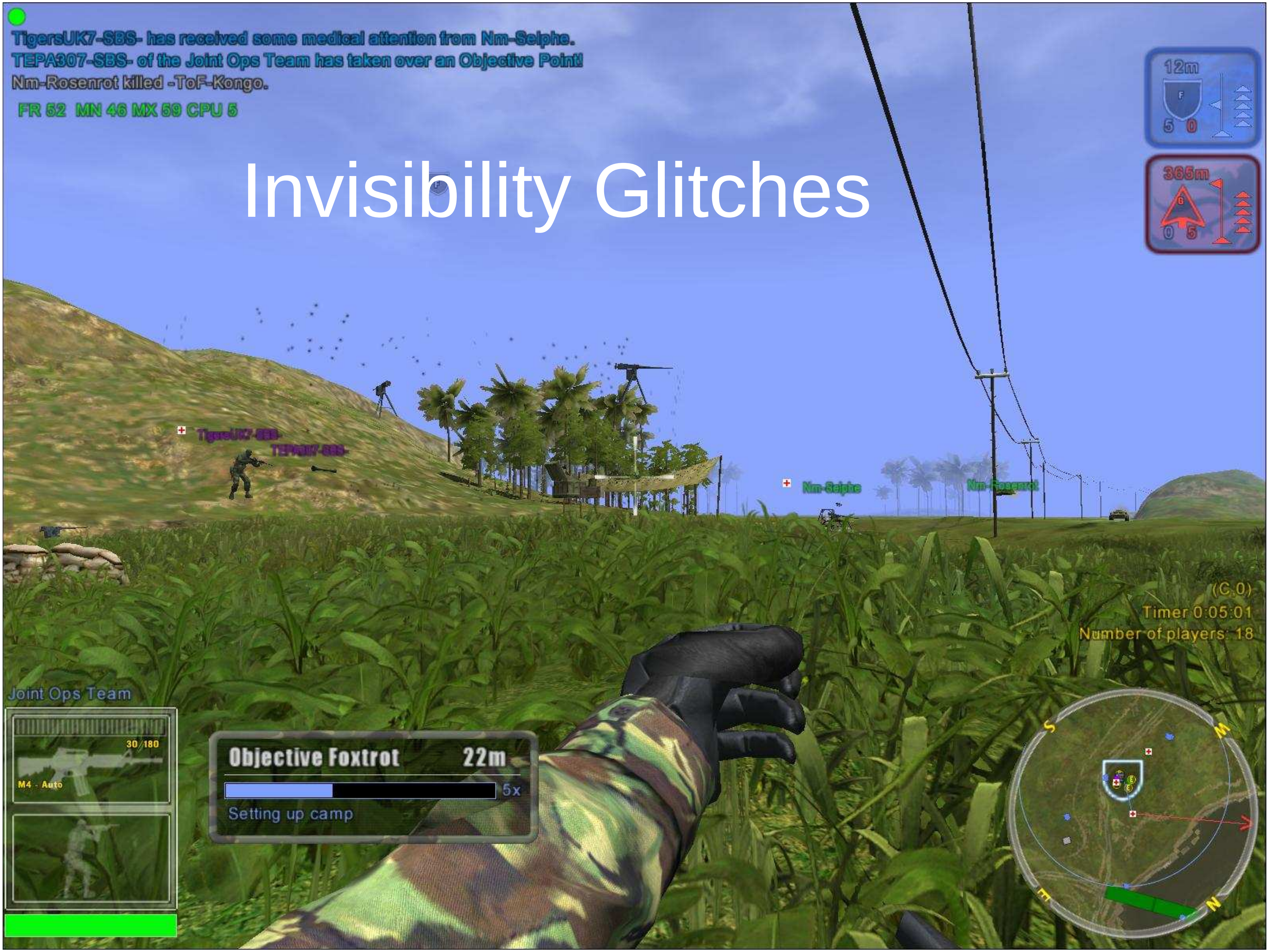
fsimon killed aiM I Twister.

Cool Box -SAS- killed BowieX.

sure the team sucks, half is sniper

MaDnIcK: cant agree more :)

Invisibility Glitches



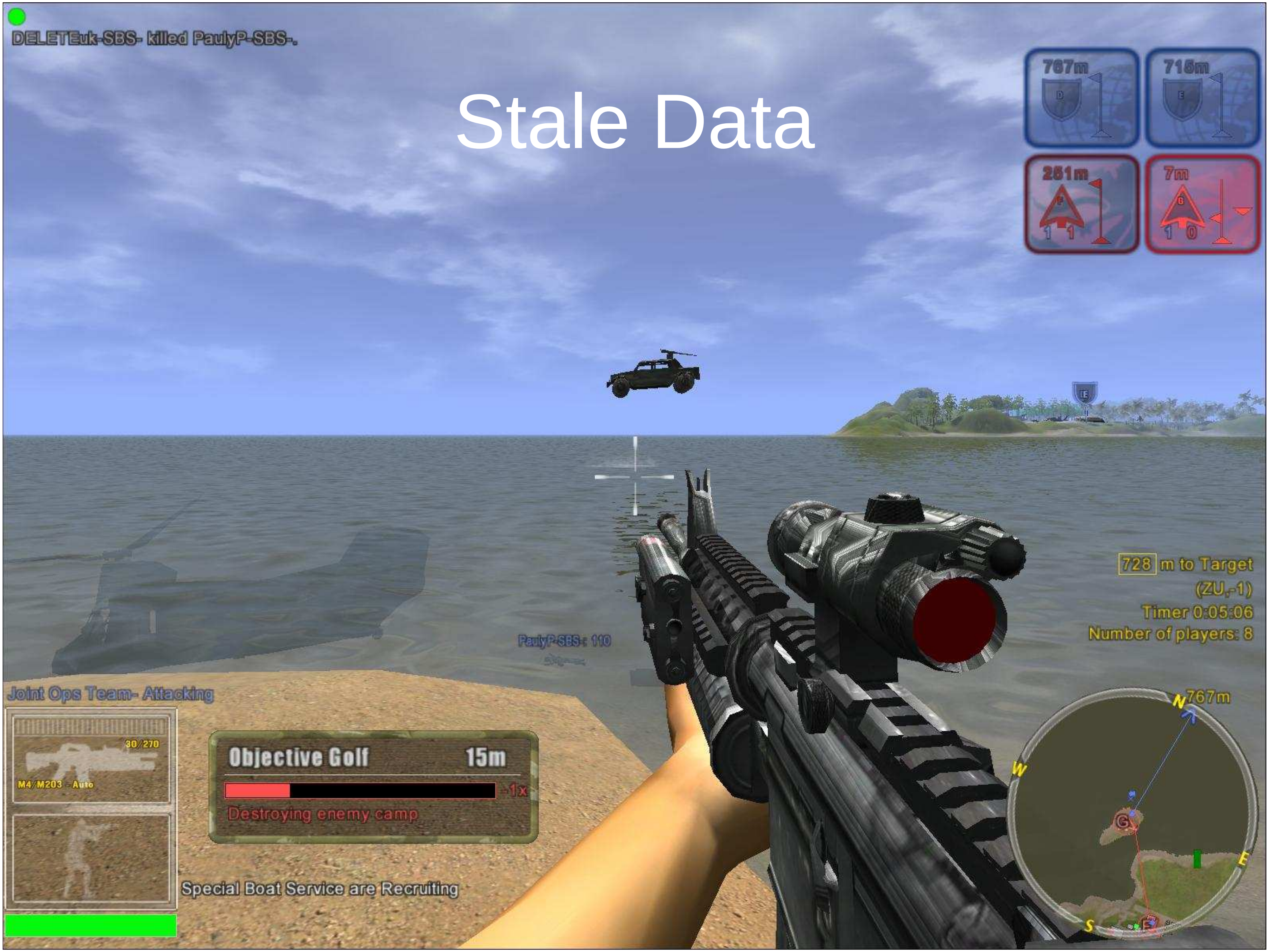
TigersUK7-SBS- has received some medical attention from Nm-Selphe.
TEPA307-SBS- of the Joint Ops Team has taken over an Objective Point!
Nm-Rosenrot killed -ToF-Kongo.

FR 52 MN 46 MX 59 CPU 5

Objective Foxtrot 22m
5x
Setting up camp

(C,0)
Timer 0:05:01
Number of players: 18

Stale Data



DELETEuk-SBS- killed PaulyP-SBS-.

728 m to Target
(ZU,-1)
Timer 0:05:06
Number of players: 8

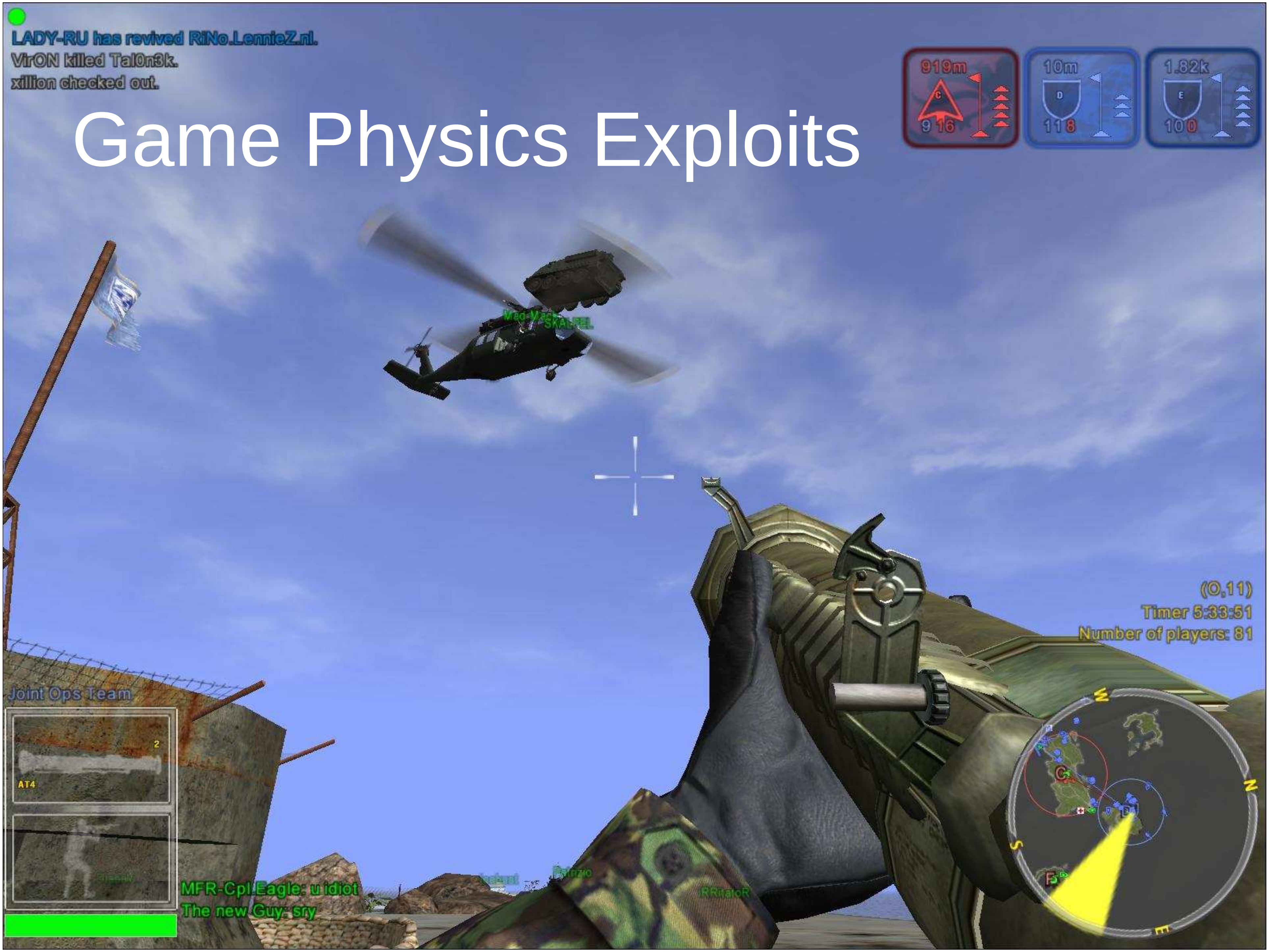
Objective Golf 15m
Destroying enemy camp

Special Boat Service are Recruiting

Deliberate Glitches and Exploits

-are considered cheating
-spoil the game for most players

Game Physics Exploits

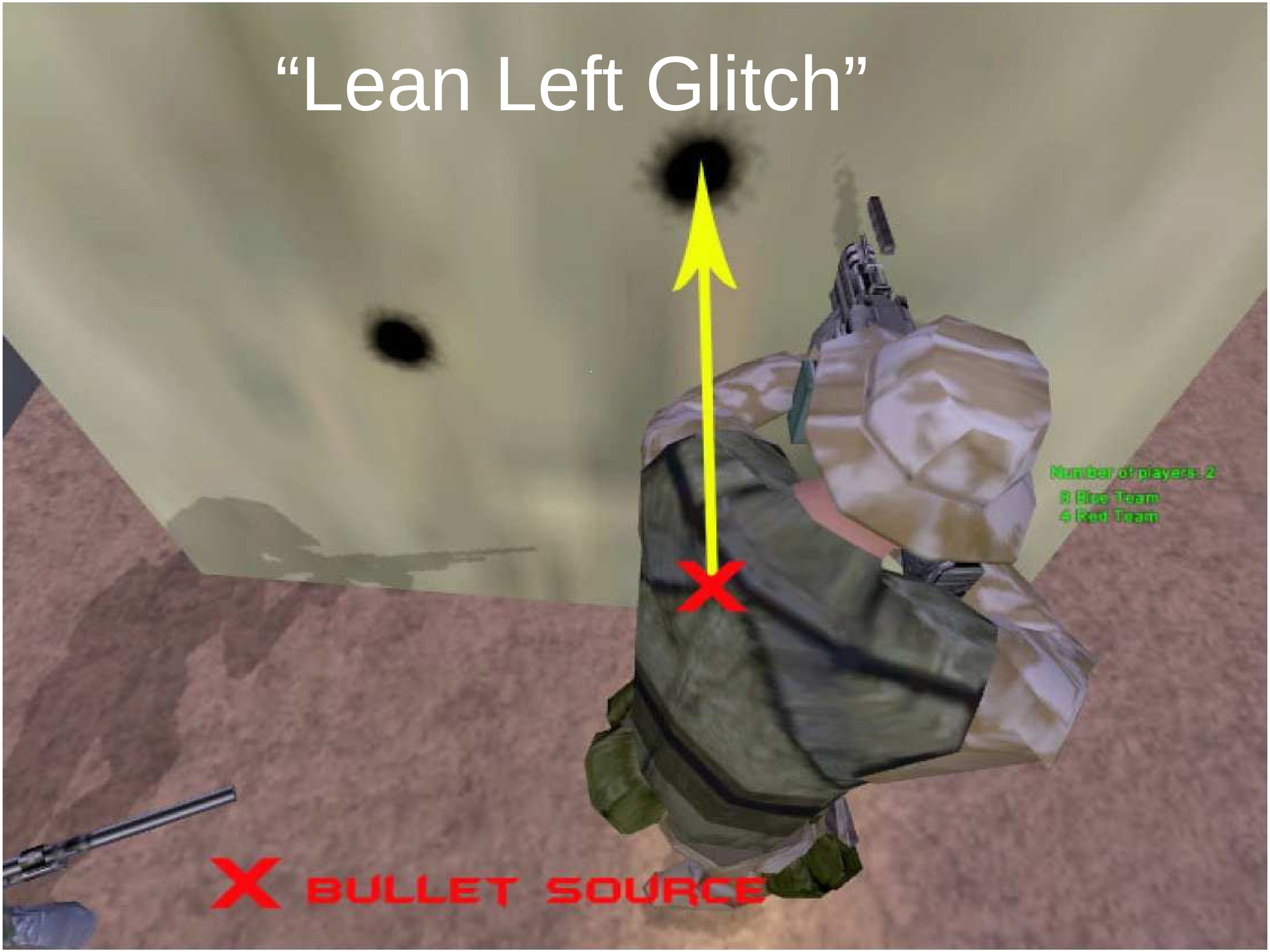


LADY-RU has revived RiNo.LennieZ.nl.
VirON killed Tal0n3k.
xillion checked out.

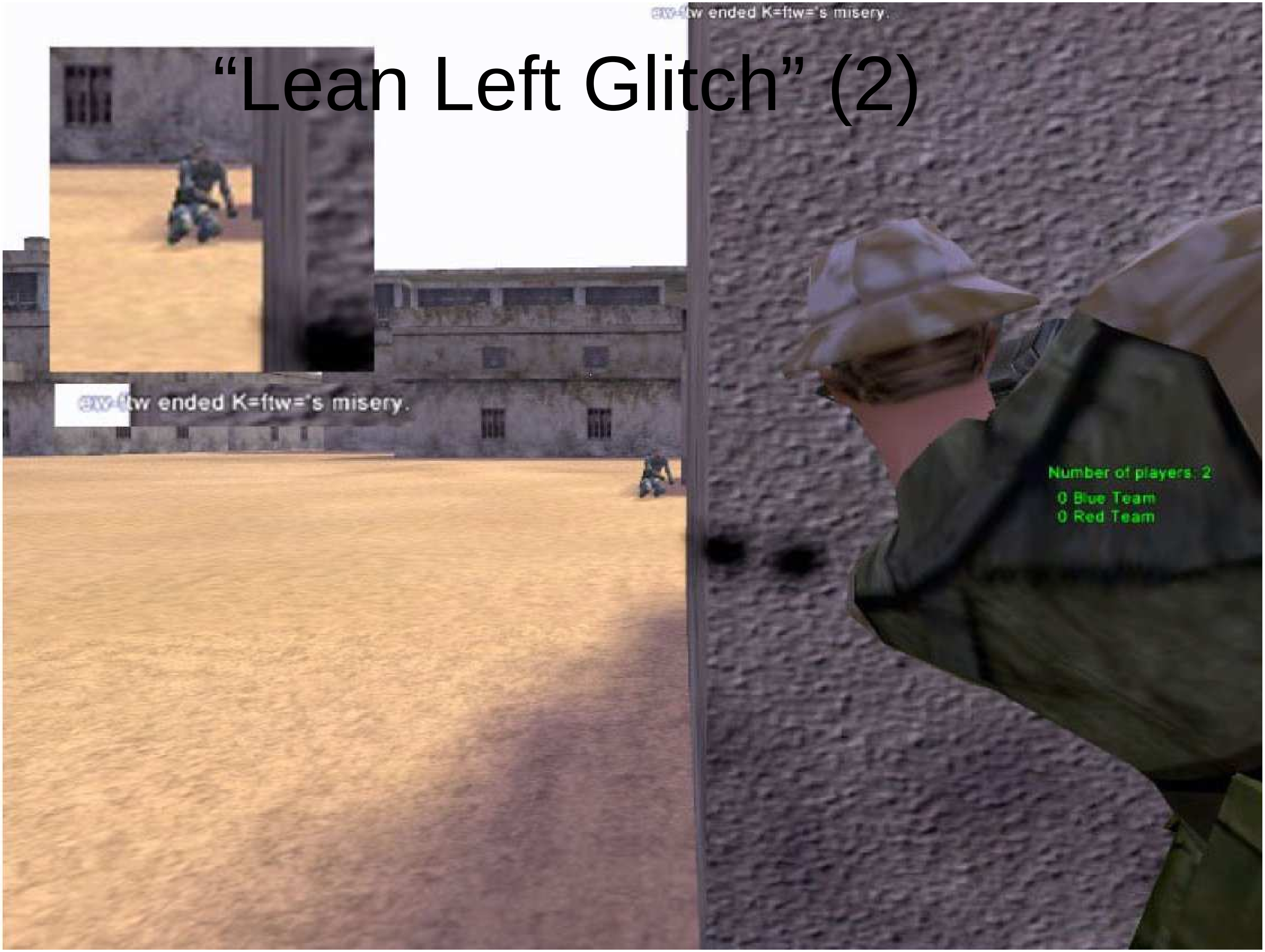
MFR-Cpl.Eagle: u idiot
The new Guy: sry

(O,11)
Timer 5:33:51
Number of players: 81

“Lean Left Glitch”



“Lean Left Glitch” (2)



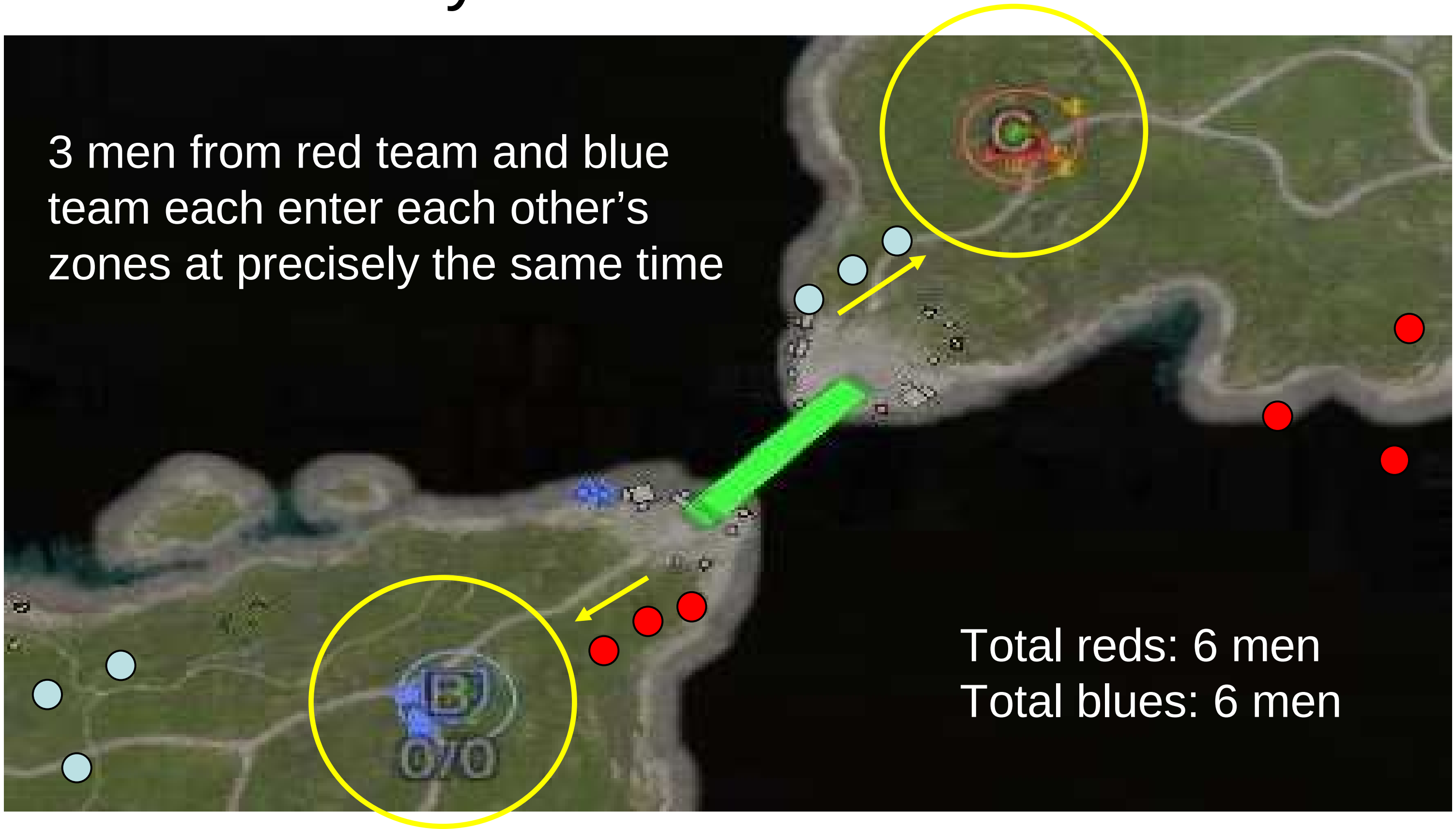
ew-ftw ended K=ftw='s misery.

ew-ftw ended K=ftw='s misery.

Number of players: 2
0 Blue Team
0 Red Team

Team Exploits

- **Cross Capture Trick.** In Advance and Secure, two teams each try to capture each other’s base simultaneously

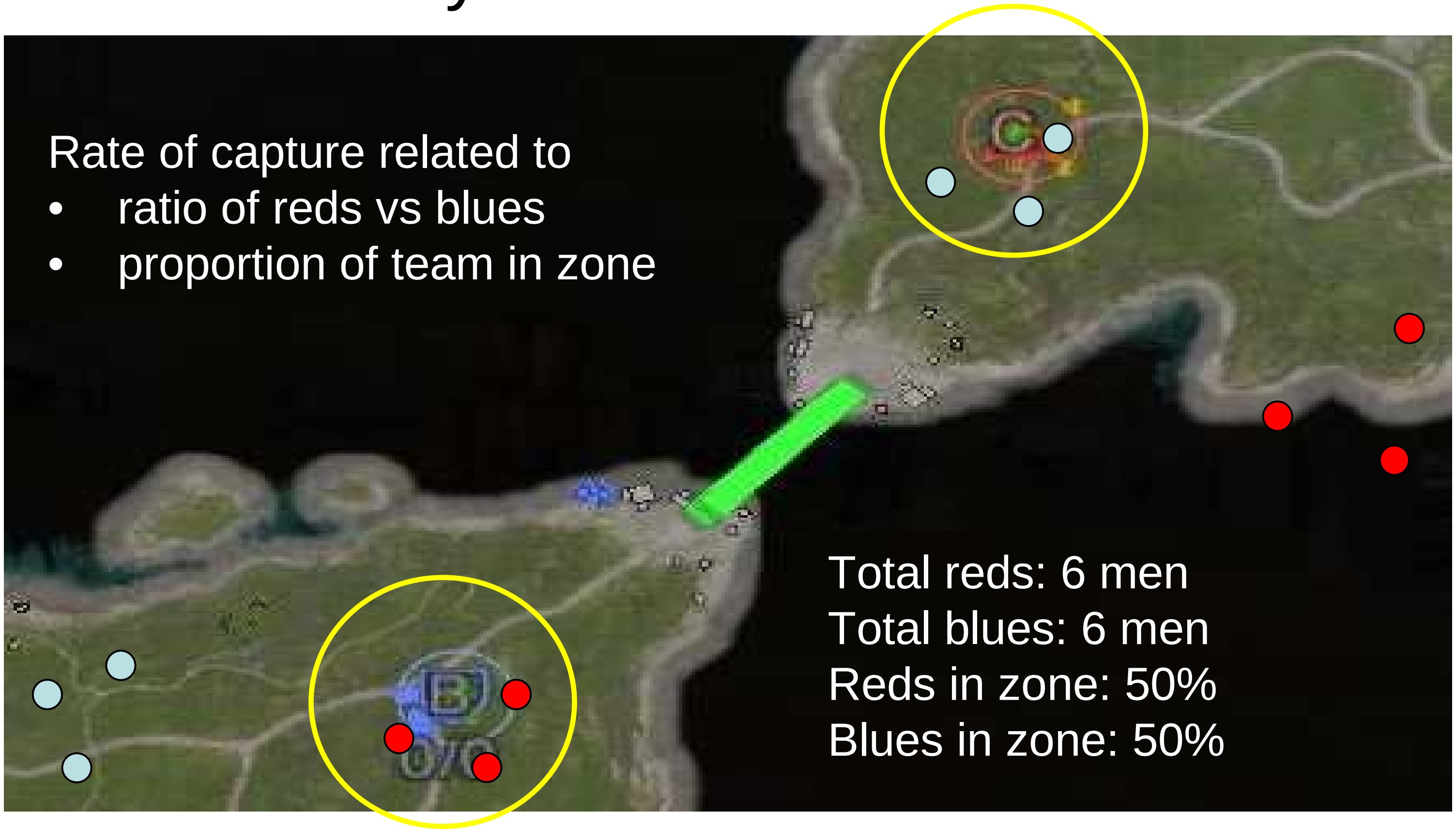


3 men from red team and blue team each enter each other’s zones at precisely the same time

Total reds: 6 men
Total blues: 6 men

Team Exploits (2)

- **Cross Capture Trick.** In Advance and Secure, two teams each try to capture each other’s base simultaneously



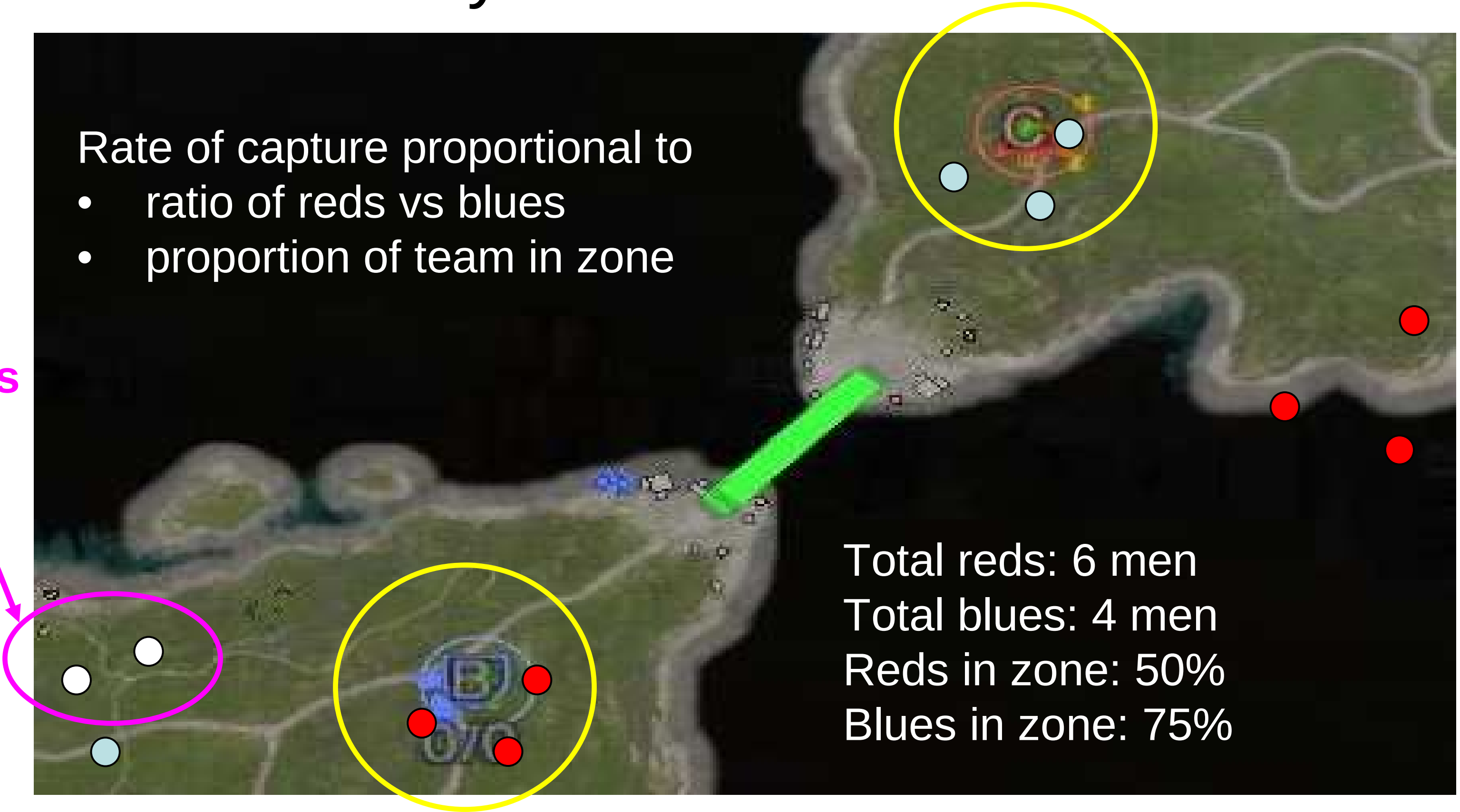
Rate of capture related to

- ratio of reds vs blues
- proportion of team in zone

Total reds: 6 men
Total blues: 6 men
Reds in zone: 50%
Blues in zone: 50%

Team Exploits (3)

- **Cross Capture Trick.** In Advance and Secure, two teams each try to capture each other's base simultaneously



Rate of capture proportional to

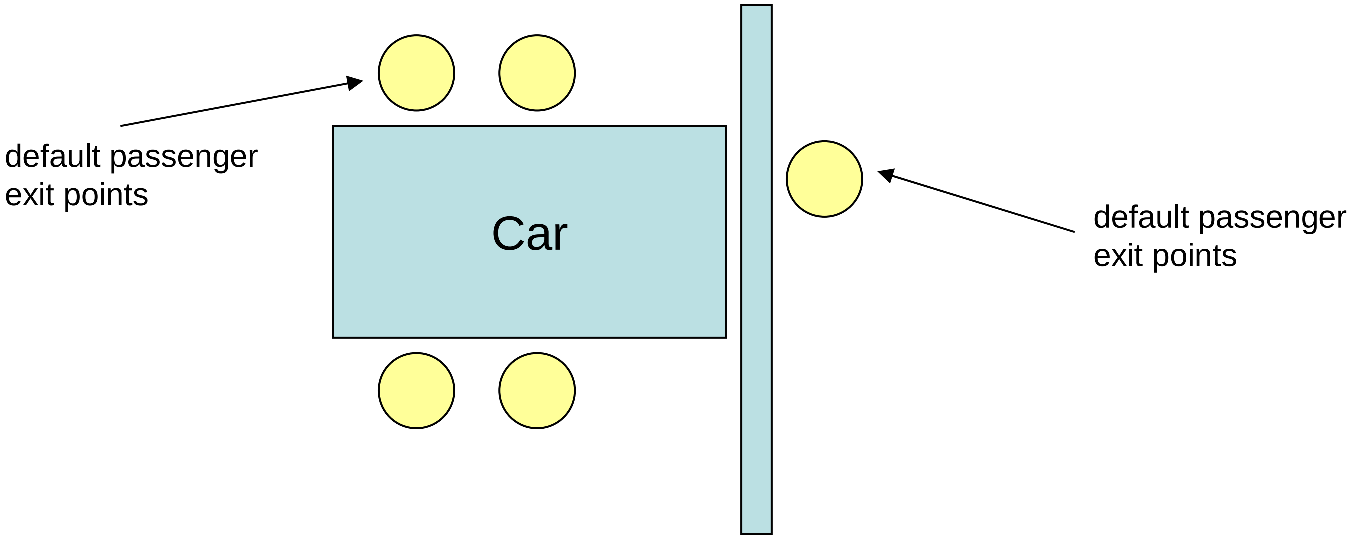
- ratio of reds vs blues
- proportion of team in zone

2 guys quit

Total reds: 6 men
Total blues: 4 men
Reds in zone: 50%
Blues in zone: 75%

Other Exploits

- **Glitching through Walls.** Drive a vehicle right up to a wall, hit the key to disemark. You appear the far side of wall.



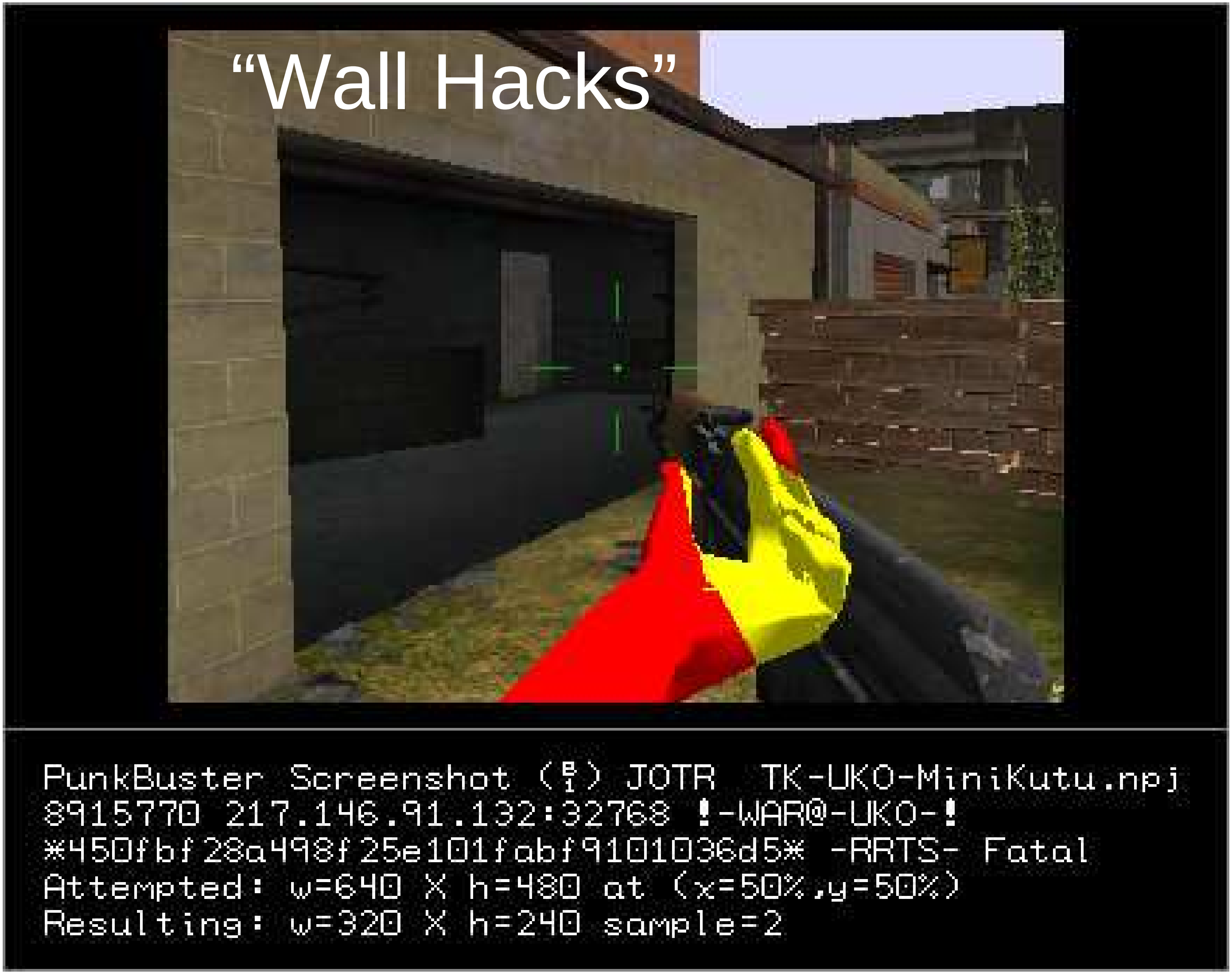
- **"Dolphin Diving"**. Constantly change posture as you move. Bullet spread is calculated based on posture, but there is no spread at all during posture change.

Good Old-Fashioned Cheating

-uses special software

-can be fought with AV-style tools

“Wall Hacks”



```
PunkBuster Screenshot (Bi) JOTR  TK-UKO-MiniKutu.npj
8915770 217.146.91.132:32768 !-WAR@-UKO-!
*450fbf28a498f25e101fabf9101036d5* -RRTS- Fatal
Attempted: w=640 X h=480 at (x=50%,y=50%)
Resulting: w=320 X h=240 sample=2
```

Subliminal Exploits
aka. “Neo-Tactics”

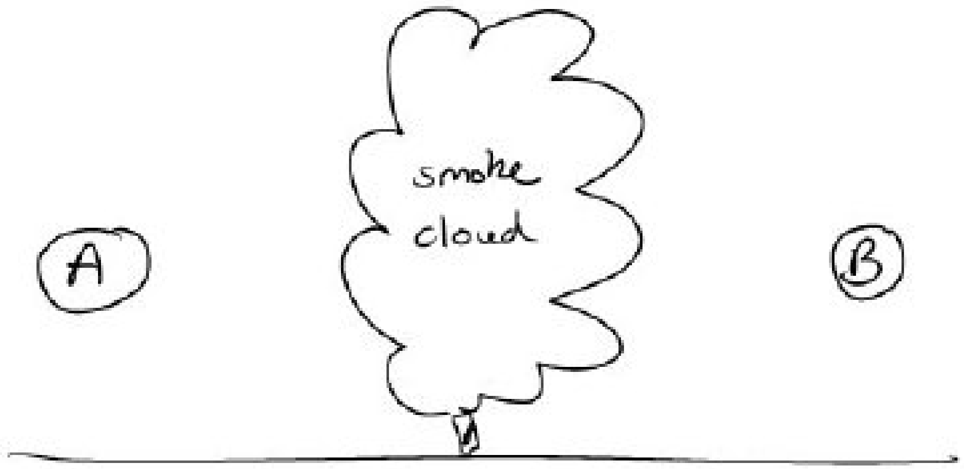
-exploit emergent game properties
-are used unwittingly by players
-are mistaken for cheating
-are “mistaken” for genius
-matter just as much as cheating

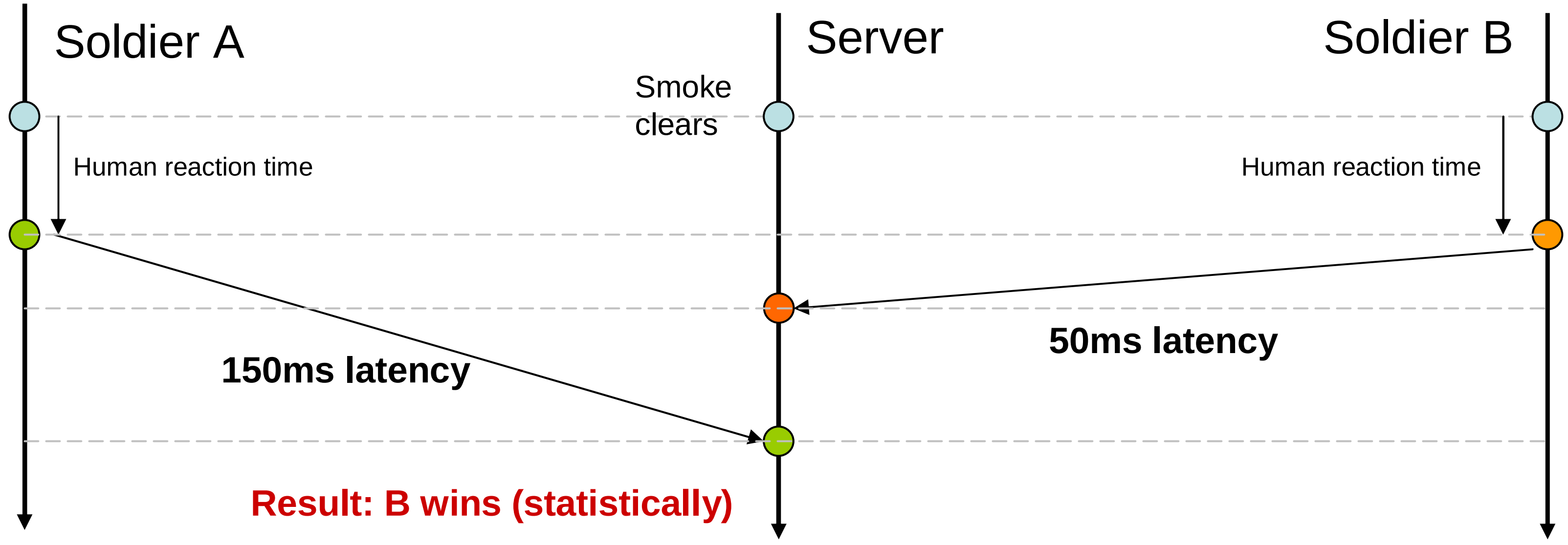
Related Work on Network Factors versus Performance

- **M.Dick, O.Wellnitz, L.Wolf "Analysis of Factors Affecting Players. Performance and Perception in Multiplayer Games",** http://www.research.ibm.com/netgames2005/papers/dick.pdf , NETGAMES 2005
- G.Armitage, "Sensitivity of Quake 3 Players to Network Latency", Poster session, SIGCOMM Internet Measurement Workshop, San Francisco, Nov 2001
- S.Zander, G.Armitage, "Empirically Measuring the QoS Sensitivity of Interactive Online Game Players", Proc Australian Telecommunications Networks and Applications Conference (ATNAC 2004), Sydney, December 2004
- Ubicom Inc, "OPScore: A Metric for Playability of Online Games with Network Impairments", http://gamer.ubicom.com/pdfs/whitepapers/IP3K-DWP-OPSCORE-10.pdf
- **Y.W. Bernier, "Latency Compensating Methods in Client/Server In-game Protocol Design and Optimization", Valve Inc**

First Shooter Advantage

1. Soldiers A & B face off, with a smoke screen between them.
2. When the smoke clears, each sees the other and opens fire
3. Both players have equal reaction times, but different connection latencies




Soldier A

Server

Soldier B

Smoke clears

Human reaction time

Human reaction time

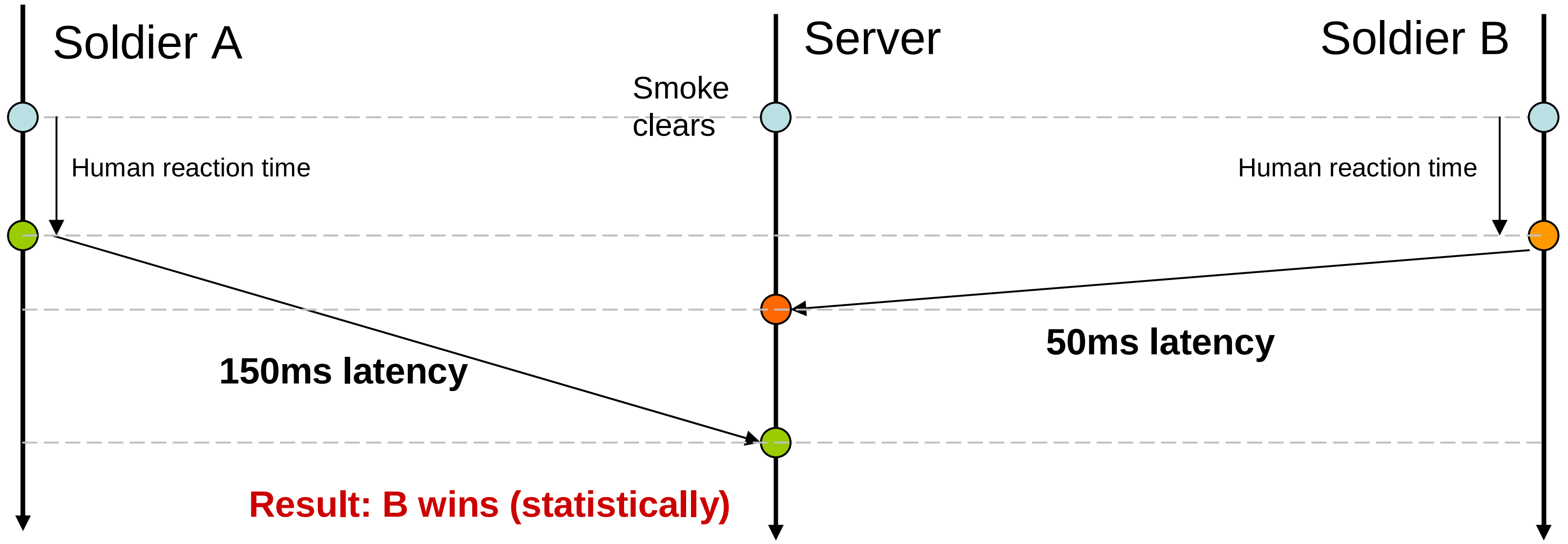
150ms latency

50ms latency

Result: B wins (statistically)

First Shooter Debunked

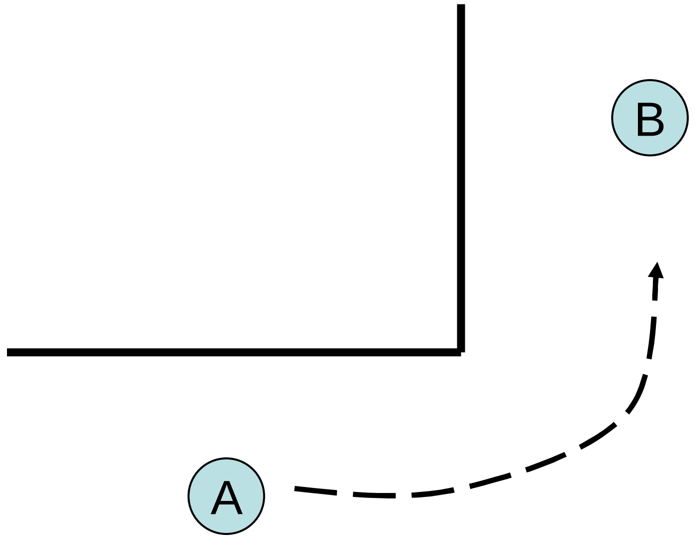
- In tactical shooters, people rarely react to a central synchronised event. Instead, one player **causes** the event.



Result: B wins (statistically)

First Mover Advantage

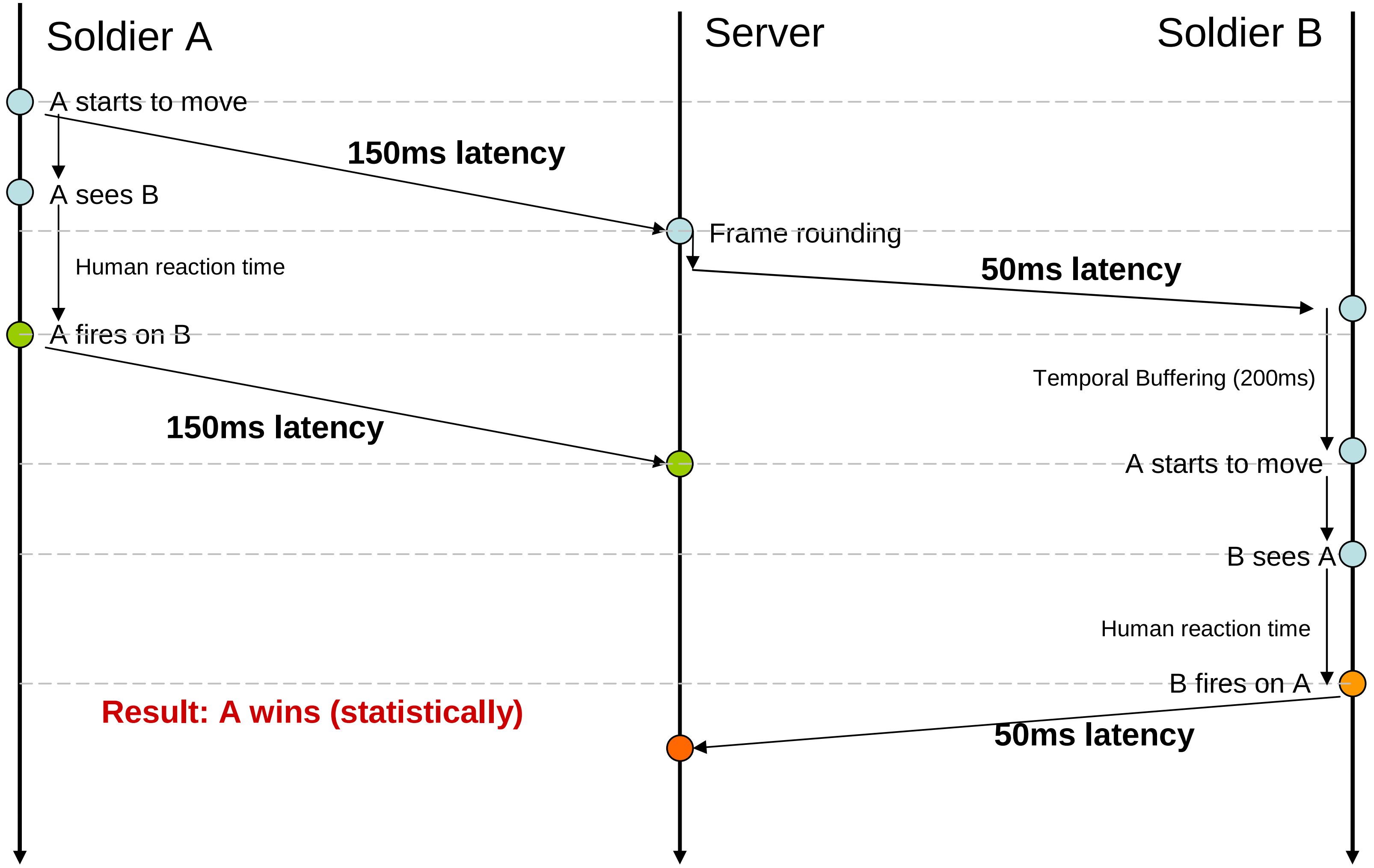
- A and B face off around a corner
- B stays still, A advances
- A gets **“client prediction benefit”** – he starts to move as soon as he pushes forward key
- A sees B first
- A has a worse ping than B
- A’s firing instructions take longer than B’s
- But A’s visual advantage outweigh this
- A wins (statistically)



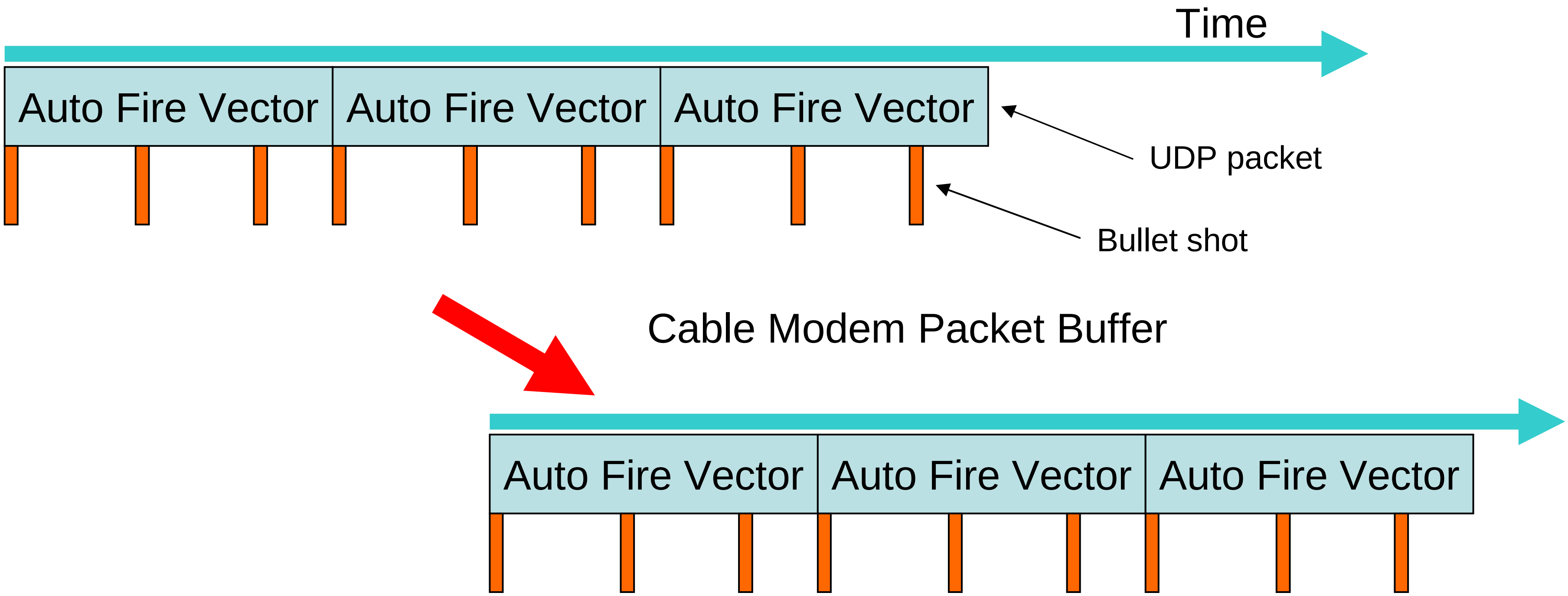
A latency :	150ms
Server proc time :	25ms
B latency :	50ms
Client temporal buffering:	200ms

B sees A after 150+25+50+200=425ms
A sees B instantly, can shoot after 150ms

First Mover Advantage (2)



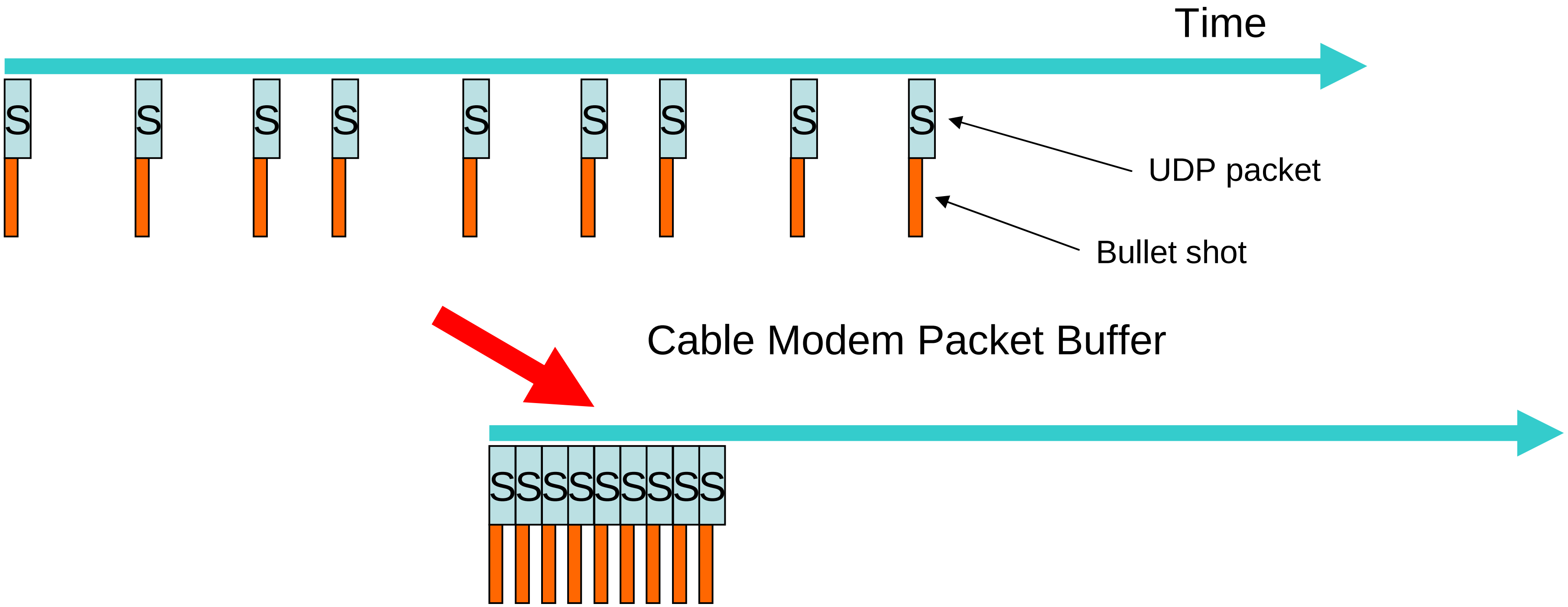
Semi-Auto Advantage



Auto-fire is a vector… spread 3 bullets along a path between A->B at 0.3 second intervals

Result: Packets take time to execute, cannot be compressed

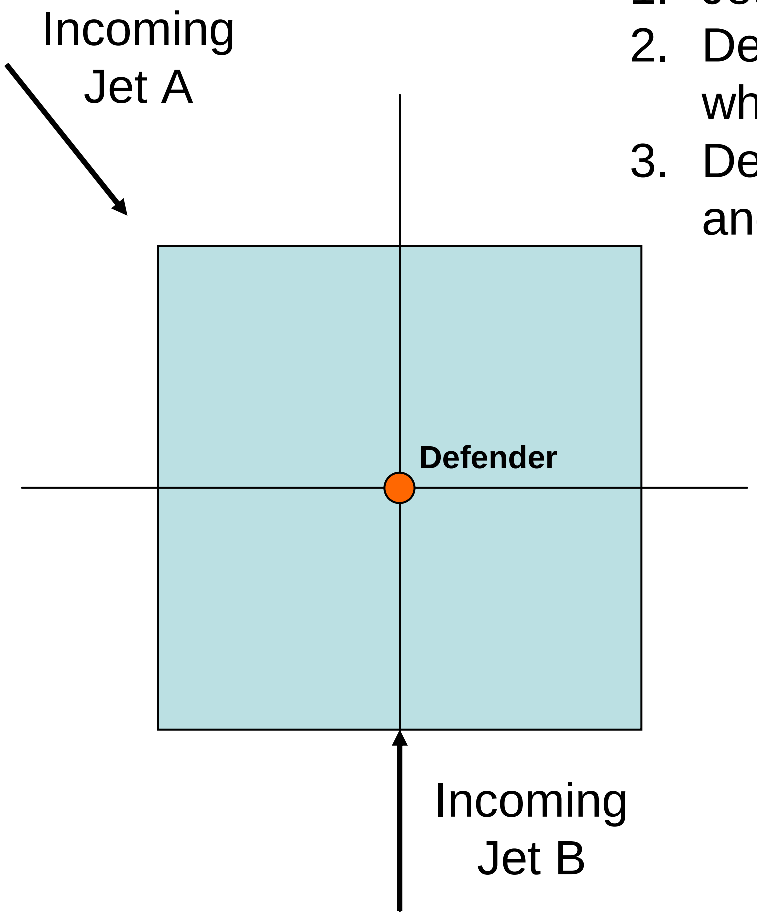
Semi-Auto Advantage (2)



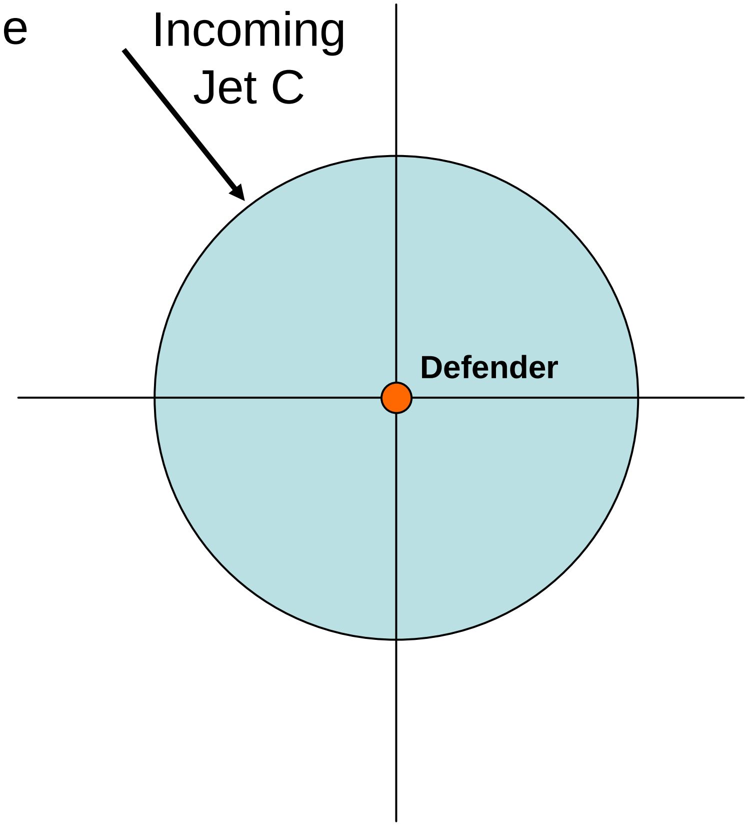
Semi-auto is a point… fire one bullet at point A, instantly

Result: Packets can be acted on instantly, so compress during modem buffering under laggy conditions (when buffer full)

Quantised Approach Advantage



1. Jet Approaches
2. Defender hears jet when it enters range
3. Defender aims and fires stinger

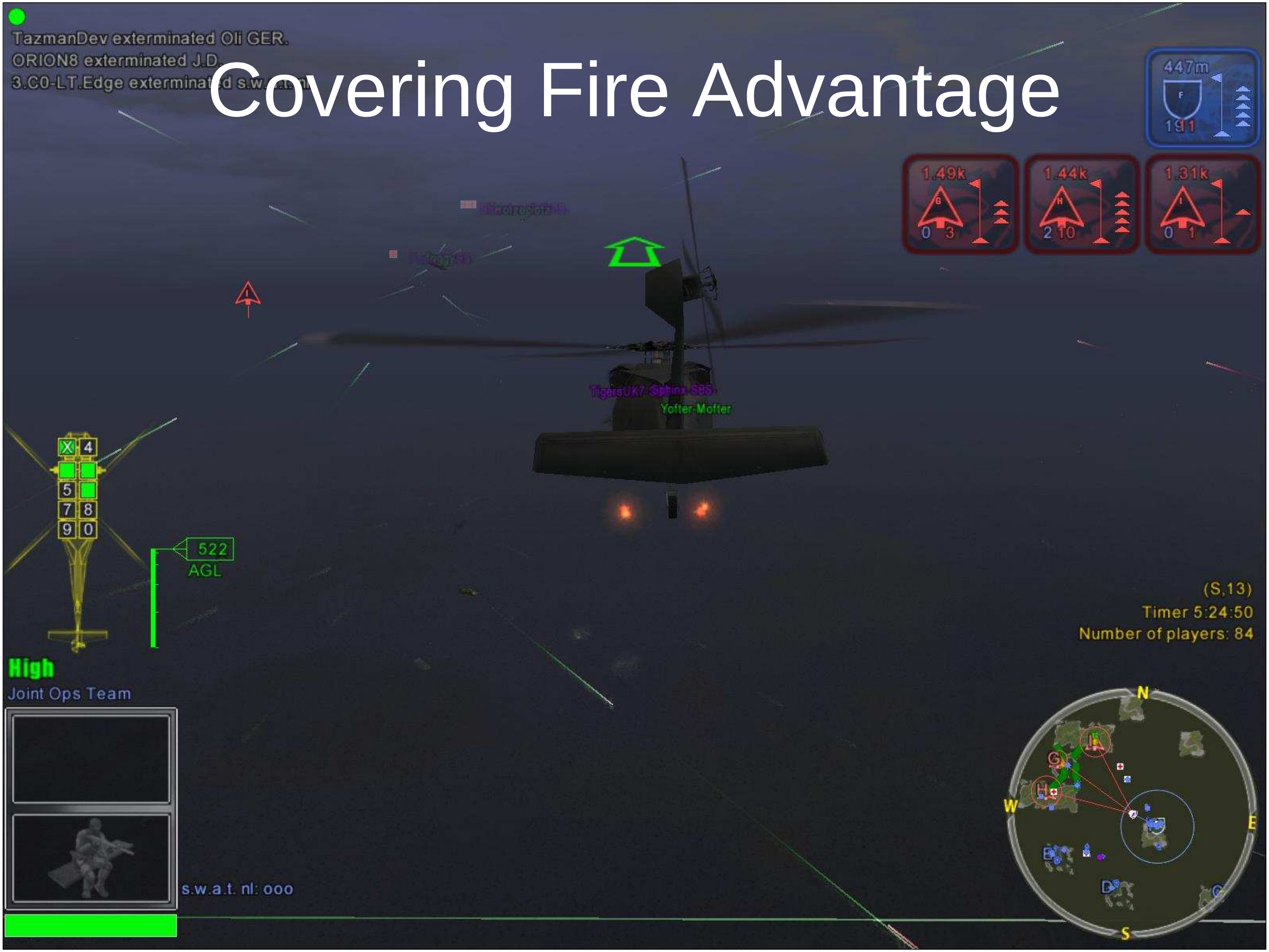


Moral: Attack from the points of the compass

Where did all the screen shots go?

- This stuff is usually too subtle to photograph
- If it was obvious, it would already be well understood
- Does industry know about it?
- Does it actually exist?

Covering Fire Advantage



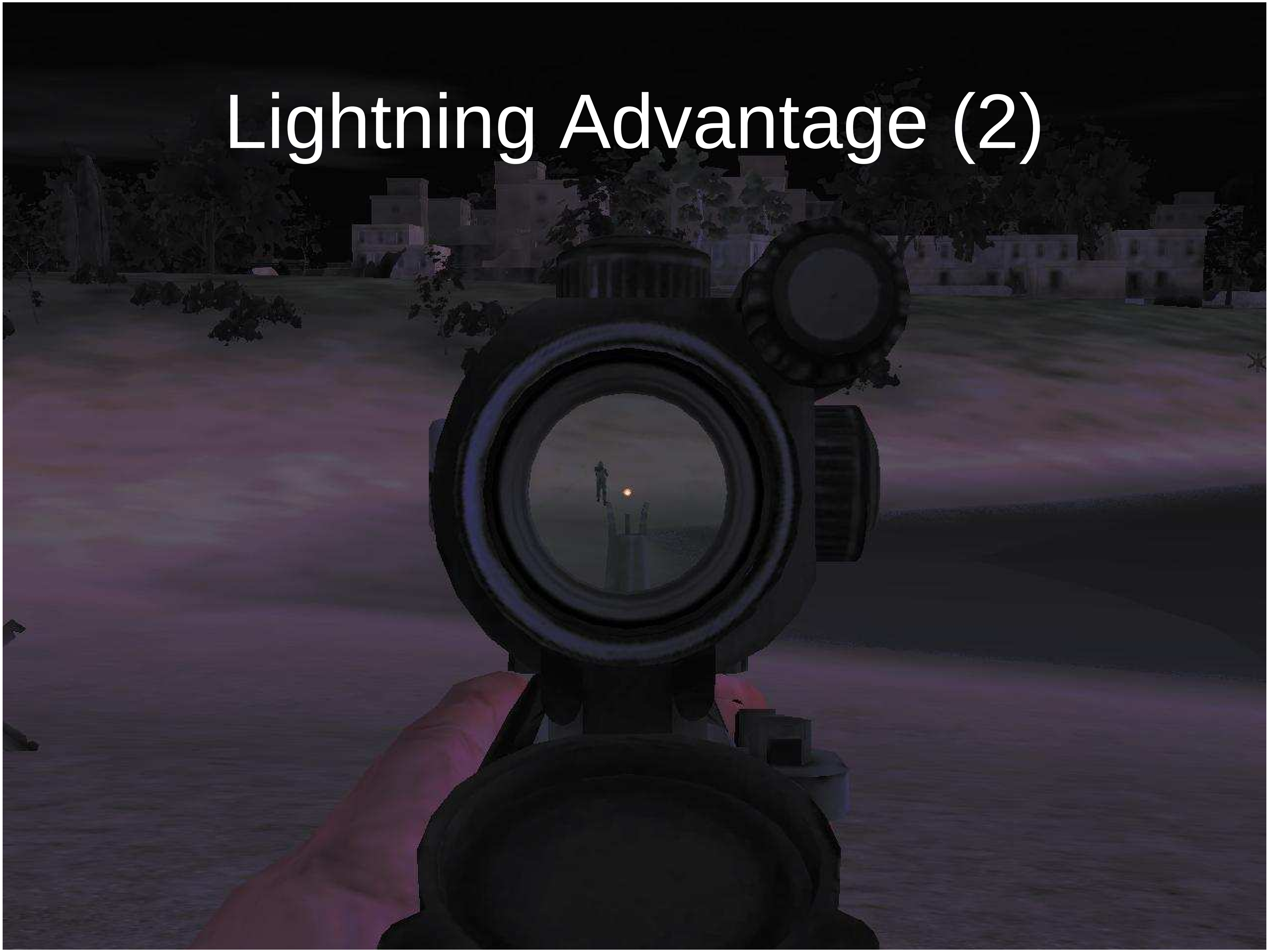
TazmanDev exterminated Oli GER.
ORION8 exterminated J.D.
3.C0-LT.Edge exterminated s.w.a.t. nl

(S,13)
Timer 5:24:50
Number of players: 84

s.w.a.t. nl: ooo

Lightning Advantage

Lightning Advantage (2)



Lightning Advantage (3)

Studying Online Gaming

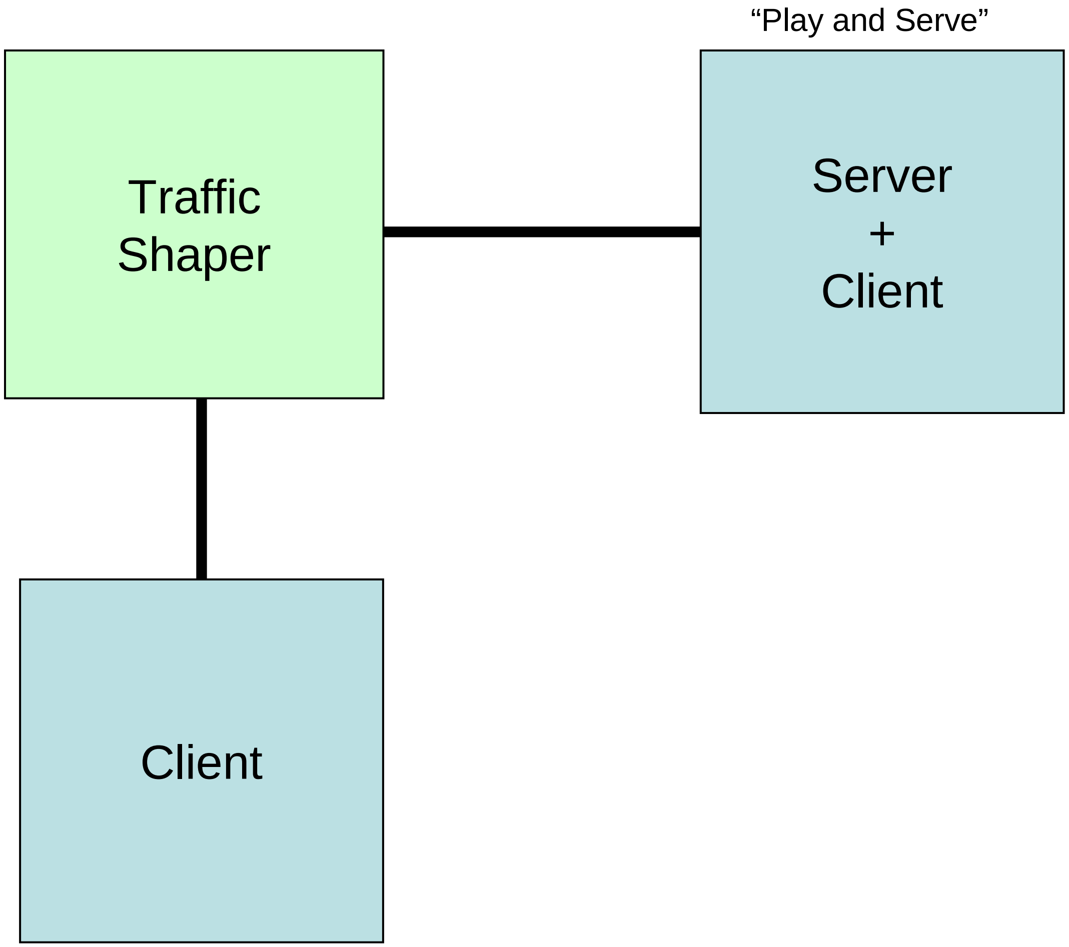
- Is hard
- It’s the real world out there
  - you can’t just hit pause
  - recruiting 64 players who will do what they’re told?
  - you need access to experienced players not novices
  - you need realistic network conditions (cable modems not academic network links)
- The community doesn’t welcome discussion of cheating methods (game dev driven taboo)
- Live experiments may fall foul of anti-cheating detection software (Punkbuster)

Getting the NetCode

- Game developers are legendarily secretive. They work for 5 years in secret on some game.
- NetCode is a games dev's crown jewels… it's the core IP about how a company makes their game playable
- There are one or two open source netcode stacks. But you need it for **Tactical Shooters**, not for arcade. They work totally differently (movement speed range is an order of magnitude larger)
- Novalogic never even debugged their own NetCode properly after introducing a patch with new vehicles (motorbikes/choppers)
- But no… I haven't tried asking anyway. I probably should

My Testing Configuration

Bandwidth Limits
Upstream Latency
Downstream Latency
Packet Loss



“Play and Serve”

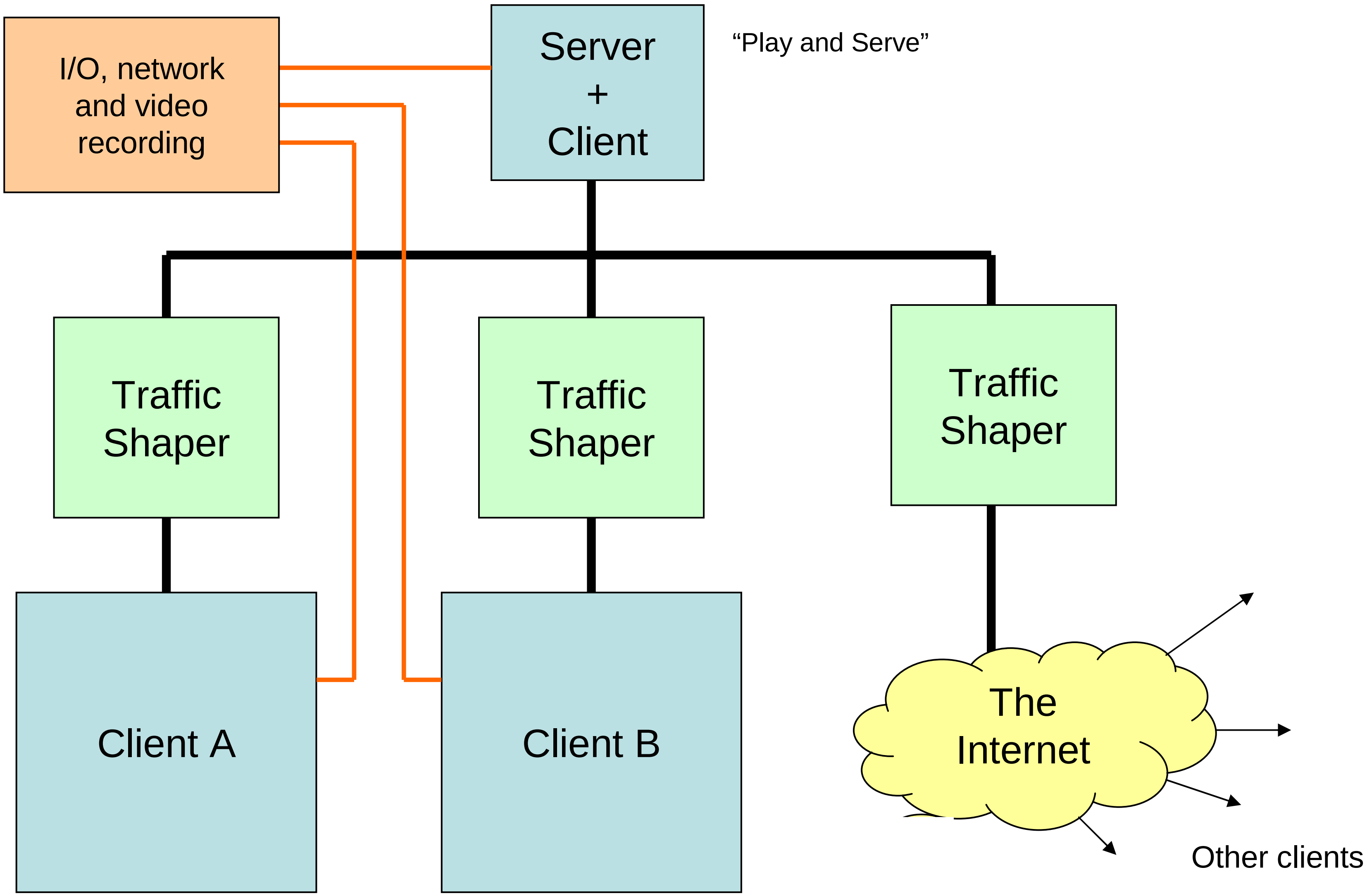
Traffic Shaper

Server
+
Client

Client

Experiment 1:
800ms upstream
(client to server)
delay exposes first
Mover advantage
to human eye

Better Configuration



Conclusions

- The online world is a very different place to reality, strange and sinister
  - Tries to deceive you that it is consistent
  - *Breaks the fundamental assumptions of science*
  - Not even causality is sacred
- If you open your mind to understand it, you can manipulate it to your advantage (like Neo)
- Traditional study of computer game security has focussed on eliminating cheating, but the *perception of cheating* is even more important.
- There may be consequences for military use
- Is a ripe research area (and you get to play games all day!)

More Information

- Boom, Headshot!

http://www.cl.cam.ac.uk/~mkb23/research/Boom-Headshot.pdf

  - Includes literature survey
  - Includes more detailed explanation of game mechanics
  - More subliminal exploit examples

Mike.Bond@cl.cam.ac.uk